数字化网络安全新时代

2021年中国政企数字化网络安全研究报告及TOP50企业榜单（上）

亿欧智库 www.iyiou.com/research

前言

新冠疫情爆发加速了全社会数字化转型进程，远程办公、在线教育、网上直播等行业高速发展。随着数字经济时代到来，云计算、大数据、物联网等新兴技术在各行业深度应用，各行业在生产方式、商业模式、管理方式等方面发生深刻变革。

网络安全事关国家安全、社会安全，信创风口以及等保2.0等政策发布奠定了网络安全行业发展基石。而在数字化转型趋势下，政企业务模式发生变化，网络安全风险呈现多样化、复杂化、难预测化的趋势，政企亟待构建与数字化业务融合的新型网络安全体系。

因此，亿欧智库立足政企数字化现状，剖析新兴技术在各行业应用所带来的网络安全风险，探究各行业数字化网络安全需求以及厂商解决方案。从宏观政策、技术、应用三大层面分析政企数字化网络安全发展现状和未来趋势，发现网络安全高成长性赛道和未来技术热点，为关注中国网络安全产业发展的读者提供参考。

本报告核心观点：

◆基于对新兴技术成熟度判断，政企数字化网络安全将围绕**云、大数据、物联网**三大技术领域展开，这三大领域交错，成为政企网络安全底座；

◆新兴安全市场进入加速期，拉动整体网络安全市场规模增长，亿欧智库预计**2021年中国网络安全市场规模将达2017.3亿元，**2021年-2023年复合增长率达19.3%。

◆从场景落地来看，亿欧智库从**合规性需求**以及**行业数字化程度**两大维度评估，政府数字化网络安全将围绕**电子政务、智慧城市、公安**三大主要场景展开；企业数字化网络安全高成长赛道包括**金融、运营商、能源、工业制造；**

◆结合投融资分析以及专家访谈结果，未来3-5年内，**数据安全、零信任架构、云原生安全、隐私计算**将成为技术热点。

亿欧智库

目录

CONTENTS

数字化网络安全概念

Digital network security concept

2025年数字经济核心产业增加值规模超14万亿元，成经济结构优化主力军

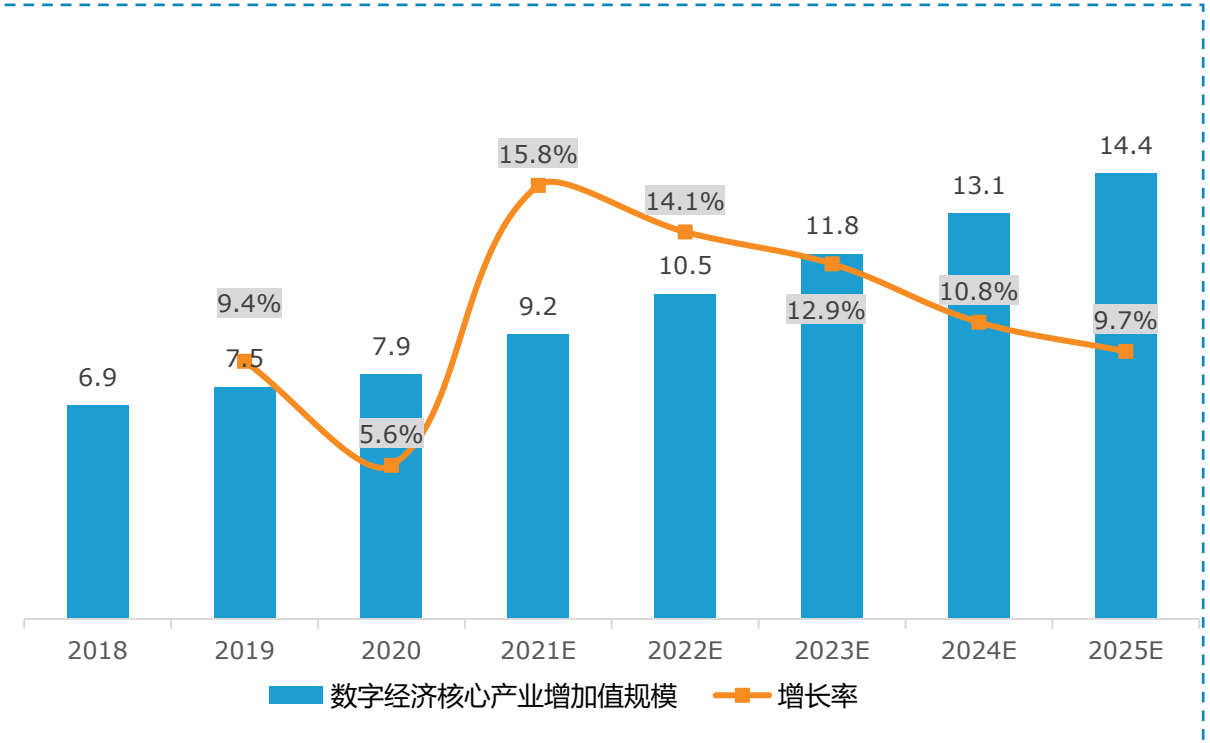
◆数字经济是指以数据资源作为关键生产要素、以现代信息网络作为重要载体、以信息技术的有效使用作为效率提升和经济结构优化的重要推动力的一系列经济活动。数字经济的出现是现代信息通信技术（ICT）大规模商业化的结果，在提高经济效率、优化经济结构上起到重要推动作用。

◆2021年6月，国家统计局发布《数字经济及其核心产业统计分类（2021）》，将数字经济产业范围确定为数字产品制造业、数字产品服务业、数字技术应用业、数字要素驱动业、数字效率提升业。其中，**除数字效率提升业之外的四大类定义为数字经济核心产业。**

◆亿欧智库测算，2025年中国数字经济核心产业增加值规模将达14.4万亿元，2021至2025年年均复合增长率为**11.9%**。

亿欧智库：数字经济产业基本范围

亿欧智库：2018-2025年中国数字经济核心产业增加值规模（单位：万亿元人民币）



来源：国家统计局、《中国经济普查年鉴（2018）》、亿欧智库整理及测算

数字化是实体经济转型新路径，新冠疫情成社会数字化“加速器”

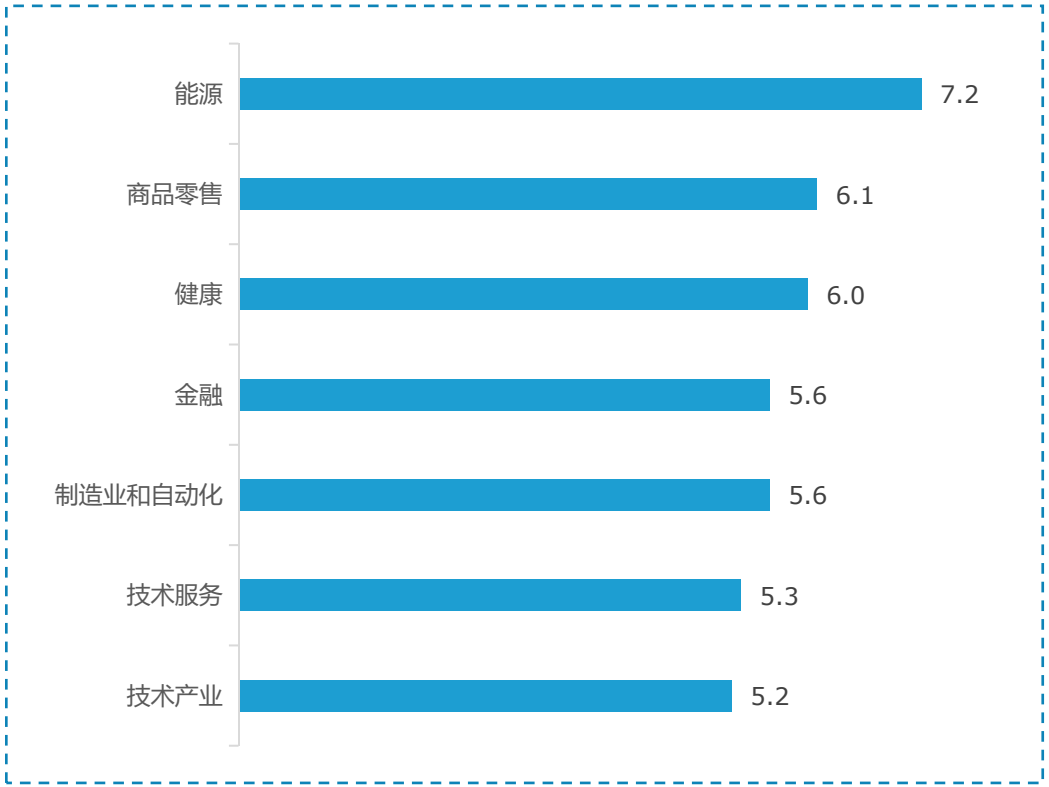
◆数字化是实体经济转型的新路径，也是数字经济的新阶段。数字化转型强调数字技术对商业的重塑，本质上是资产、运营、人力全方面的数字化，企业自身的组织形态、企业文化等都需要相应调整和变化。

◆2020年初的疫情对中国经济社会的数字化转型起着重要推动作用，网络直播、在线办公、网络会诊等数字化工具提升了各地复工复产的效率，消费者习惯养成后，后疫情时代仍保持高速发展。据云通讯公司Twilio调查数据，本次疫情将全球的数字化进程平均提前了5-7年。

亿欧智库： 2020年中国数字化转型主要政策文件

发布时间	发布单位	政策名称	主要内容
2020年8月	国务院国资委	《关于加快推进国有企业数字化转型工作的通知》	推动国有企业数字化转型做出全面部署，系统明确国有企业数字化转型的基础、方向、重点和举措
2020年10月	全国人大	《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》	迎接数字时代，激活数据要素潜能，推进网络强国建设，加快建设数字经济、数字社会、数字政府
2020年7月	发改委等13部门	《关于支持新业态新模式健康发展 激活消费市场带动扩大就业的意见》	加快推进产业数字化转型壮大实体经济新动能 。 加快传统企业数字化转型步伐 建立政府 金融机构 平台 中小微企业联动机制发展普惠性上云用数赋智
2020年5月	发改委	《数字化转型伙伴倡议》	带动中小微企业数字化转型，推行普惠性“上云用数赋智”服务，加快打造数字化企业
2020年4月	发改委 网信办	《关于推进“上云用数赋智”行动，培育新经济发展实施方案 》	大力培育数字经济新业态深入推进企业数字化转型打造数据供应链 以数据流引领物资流、 人才流、技术流 、资金流

亿欧智库：2020年疫情后中国企业数字化进程加速年份
（单位：年份）



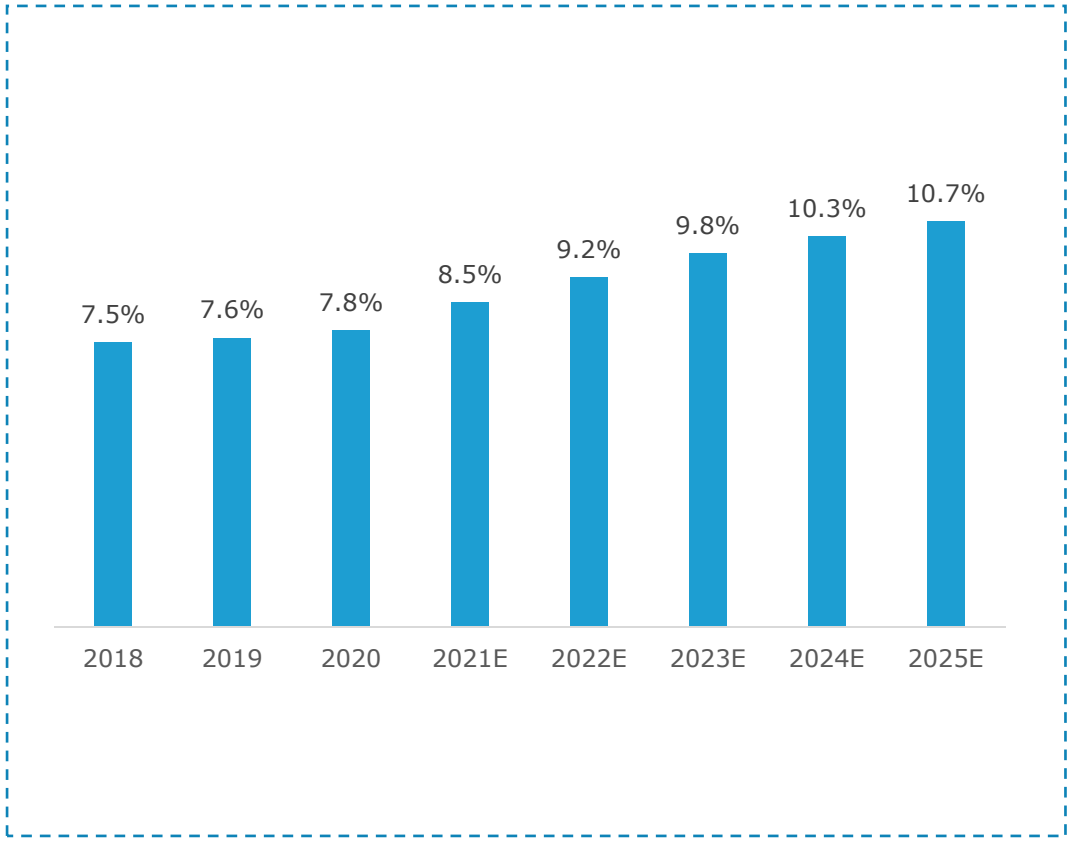
来源：Twilio、亿欧智库整理

“上云用数赋智”破解政企数字化转型难题

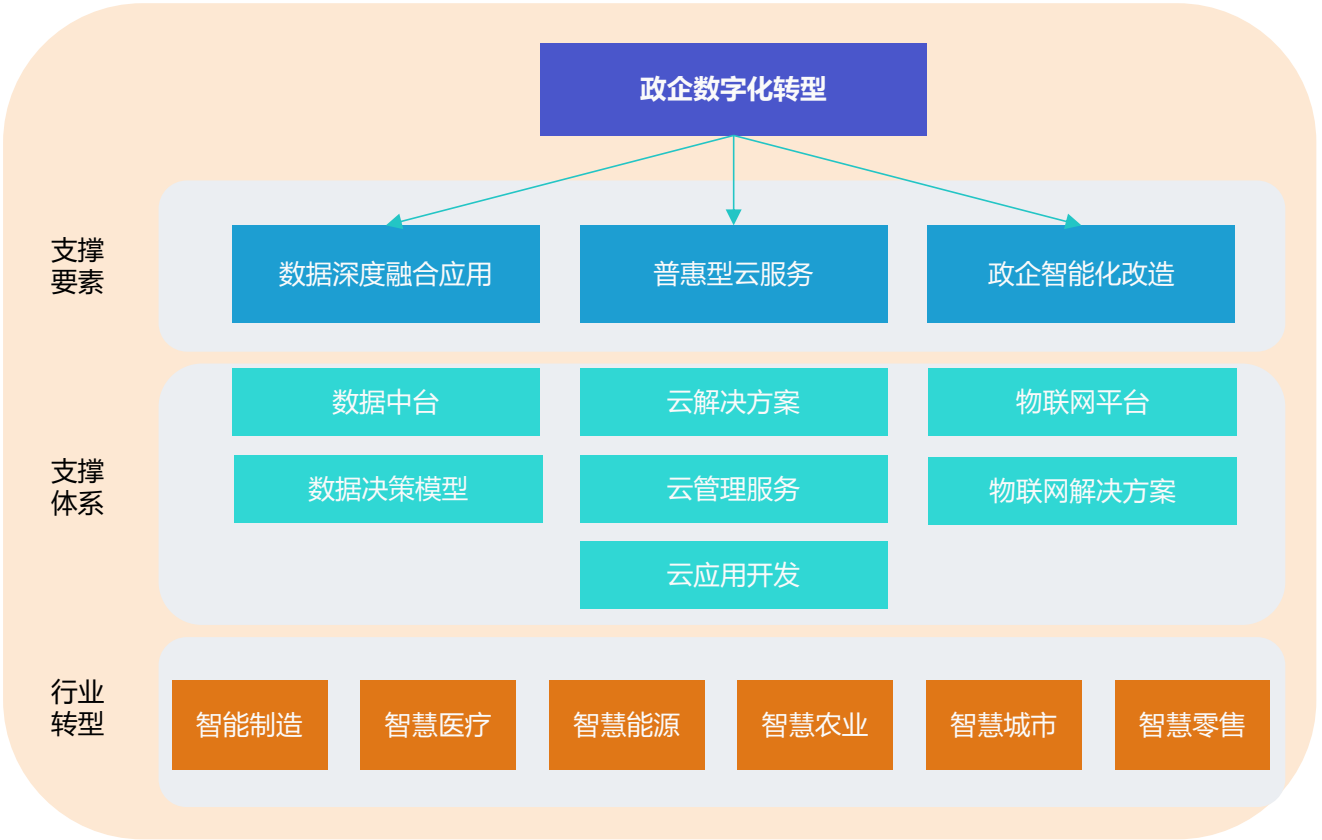
◆政企数字化转型是一场效率的革命，提升效率的关键在于：1）充分利用数据生产要素；2）充分解放云边端一体化带来的计算能力；3）充分发挥物联网等带来的智能化管理手段。2020年，国家发改委发布了《数字化转型伙伴倡议》，要求加强针对数字化转型共性解决方案的研发，探索大数据、人工智能、数字孪生、5G、工业互联网、物联网和区块链等数字技术应用和集成创新，形成更多有创新性的共性解决方案和标准。

◆亿欧智库预测，中国数字经济核心产业增加值规模占GDP将逐年提升，到2025年将提升至10.7%。

亿欧智库：2018-2025年中国数字经济核心产业增加值规模占GDP比重



亿欧智库： 政企数字化转型“上云用数赋智”路径框架



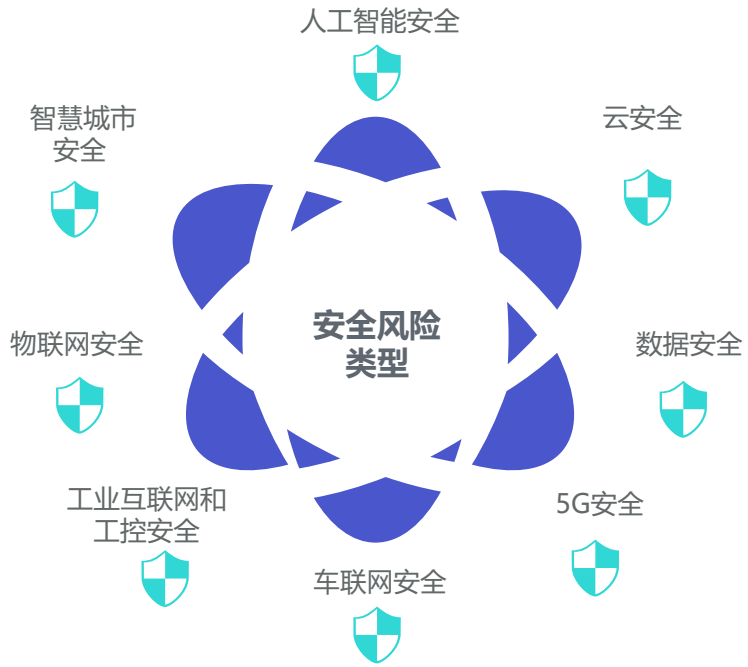
来源：国家统计局、《中国经济普查年鉴（2018）》、亿欧智库整理及测算

政企数字化转型催生众多网络安全风险，传统防护手段难以抵御

◆云计算、大数据、物联网技术的应用使网络边界日趋模糊，大数据技术的发展，使数据储量和流量成倍上涨，网络安全攻击带来的损失和伤害也随之成倍增加；物联网打通了线上线下的界限，利用设备漏洞控制物联网甚至可对物理世界造成伤害；云计算模糊了传统的安全边界，安全建设前移将成为趋势，安全攻防的复杂程度也大大增加。

◆传统“头痛医头、脚痛医脚”的网安产品布局方式逐渐无法满足用户需求，政企对于数字化网络安全建设需求提升，平台型、系统性、体系化的网络安全建设成为其关注重点。

亿欧智库：数字网络安全时代安全风险类型



亿欧智库：传统网络安全防护无法解决数字化转型中的网络安全问题

传统安全防护核心要点	传统安全防护无法解决的问题
边界安全：内外网隔离，内网绝对安全	边界逐渐模糊：云计算的高速发展，企业上云的大背景下，整个企业的网络边界的定义不再绝对
账户安全：通过账户认证后获取绝对信任，授予相应权限	账户不再安全：当前网络攻击技术手段持续提升，攻击逐渐智能化体系化；80%的数据泄露来自于内部人员的误操作或蓄意泄露
网络安全行业：以“头痛医头、脚痛医脚”的方式进行产品布局，未能产生体系化。	网络安全行业：IT基础设施重要性增强，需要平台型、系统型、体系化的网络安全措施

来源：工信部、亿欧智库整理

经过四个时代的阶段性发展，网络安全进入“大安全”时代

◆**通信加密时代，1940-1994年：**从战时通信加密技术演化而来，网络安全处于萌芽状态，仅有政府零星组织防计算机病毒及犯罪的工作。

◆**PC安全时代，1994至 2004年**：个人电脑普及，网络安全关注设备本身，防病毒产品、终端杀毒软件是主要的产品形态。

◆**信息安全时代，2004-2013 年：**移动互联网普及，网络安全关注转移到网络边界和办公信息。

◆**数字网络安全时代，2014 年至今：**智能化技术兴起，安全边界模糊，网安强调安全解决方案和安全服务，进入数字网络安全时代。

亿欧智库：中国网络安全发展历程

	1940 至 1994年	1994 至2003年	2004至2013年	2014年至今
	战时通信加密	PC安全时代	信息安全时代	数字网络安全时代
核心需求	以军用国防需求为主 尚未出现民用市场	围绕PC设备的防病毒产品 终端杀毒软件	内外网隔离的网络边界安全 面向信息化办公的信息安全	基于整体业务场景的 安全解决方案和安全服务
政策驱动	——	《中华人民共和国计算机信息系统安全保护条例》	《国家信息化领导小组关于加强信息安全保障工作的意见》	《中华人民共和国网络安全法》 《网络安全等级保护条例》 《数据安全法》
市场驱动	——	个人电脑和互联网加速渗透 门户开始网站崛起	计算机和互联网全面普及 企业信息化和政务信息化发展 移动互联网迅速升级	数字化转型全面启动 新基建使网络架构全面升级 旧的网安措施难以满足新时代需求
技术积累	密码学、通信加密学	防病毒技术、特征库、黑名单技术 电子数据加密、备份与恢复	网络隔离、网络分域/分区、身份验证、 访问控制、虚拟专用网络 (VPN)、文档 加密、应用安全、身份安全等	数据安全技术、云安全技术 IOT安全技术、隐私计算技术等
代表企业	——	国内：冠群金辰、瑞星、江民、360 国际：诺顿、迈克菲、趋势科技、卡巴斯基	天融信、绿盟、启明星辰、奇安信	网络安全类初创企业等

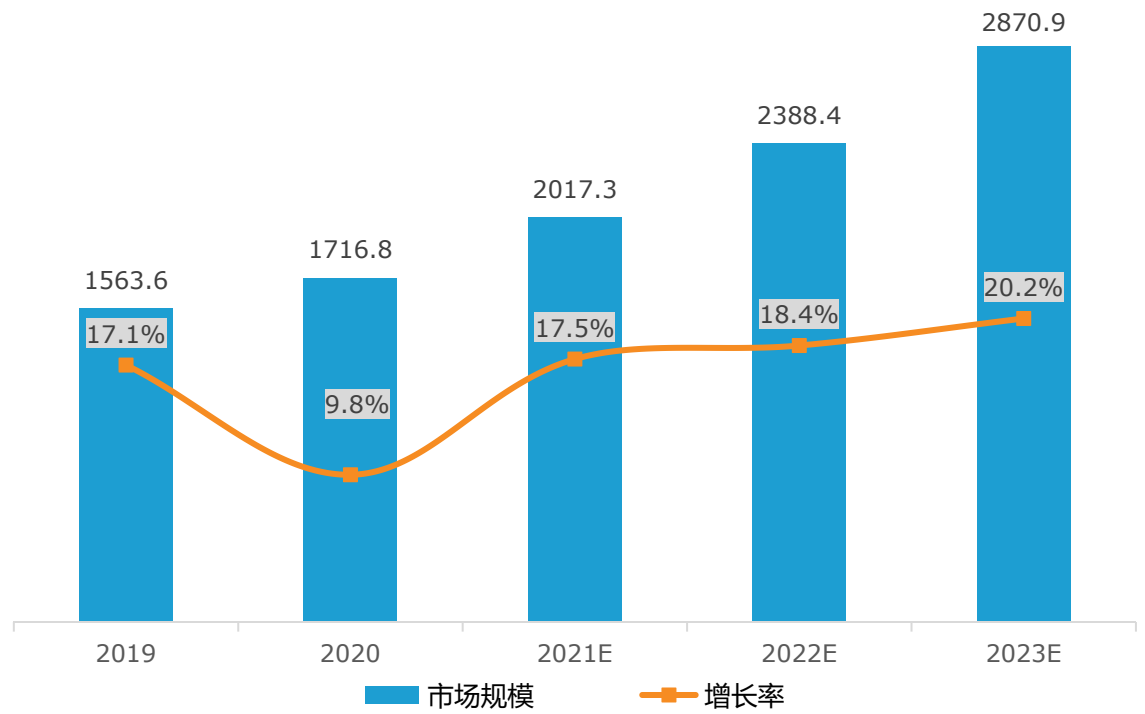
来源：亿欧智库整理

2021年中国网络安全市场超2000亿元，2021-2023年复合增长率达19.3%

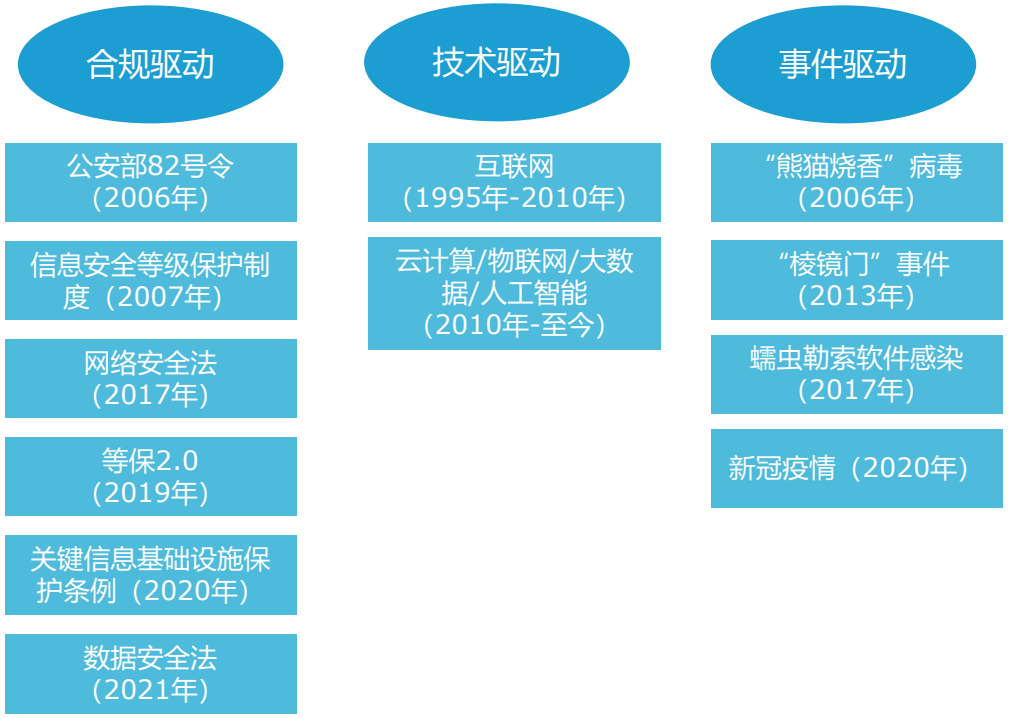
◆网络安全行业主要受到合规驱动、技术驱动以及事件驱动影响。随着2019年12月等保2.0正式实施，以及各类新兴技术在各行业落地应用，网络安全行业迎来了高速增长。传统网络安全产品受等保驱动保持稳健增长态势，新兴安全市场进入加速期，拉动整体网络安全市场规模增长。亿欧智库测算，2021年中国网络安全市场将达2017.3亿元，2023年将超2500亿元，2021-2023年复合增长率达19.3%。

◆新冠疫情虽然影响了国家整体商业活动进行，但是各行业加速数字化给网络安全行业带来了全新机遇，远程办公推动了零信任发展，在线教育、在线购物拉动了云安全等领域需求。

亿欧智库：2019-2023年中国网络安全市场规模
（单位：亿元人民币）



亿欧智库：中国网络安全市场发展驱动因素

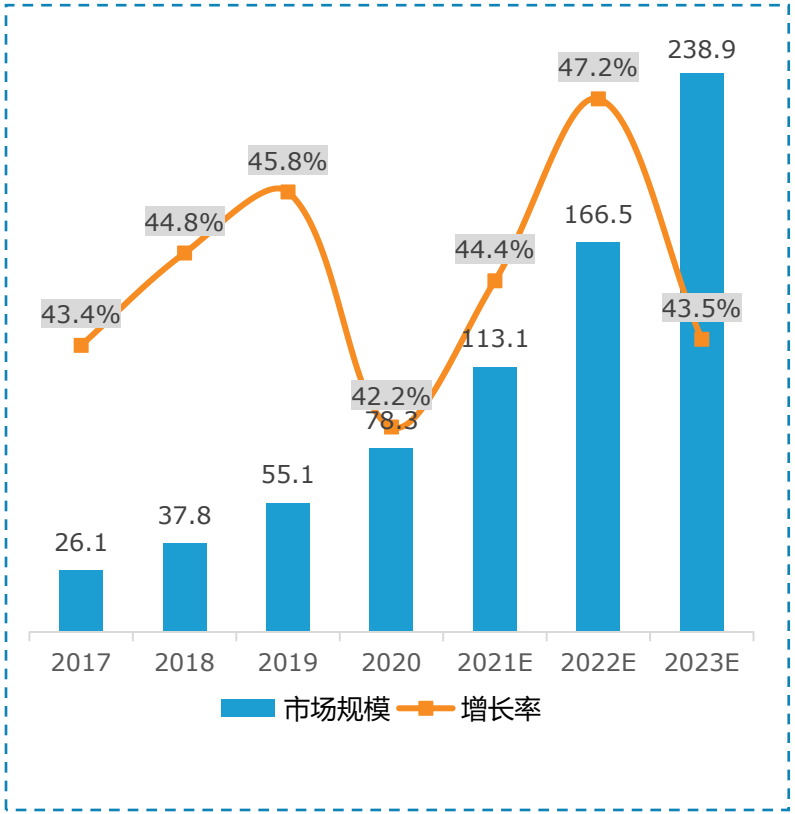


来源：专家访谈、亿欧智库整理及测算

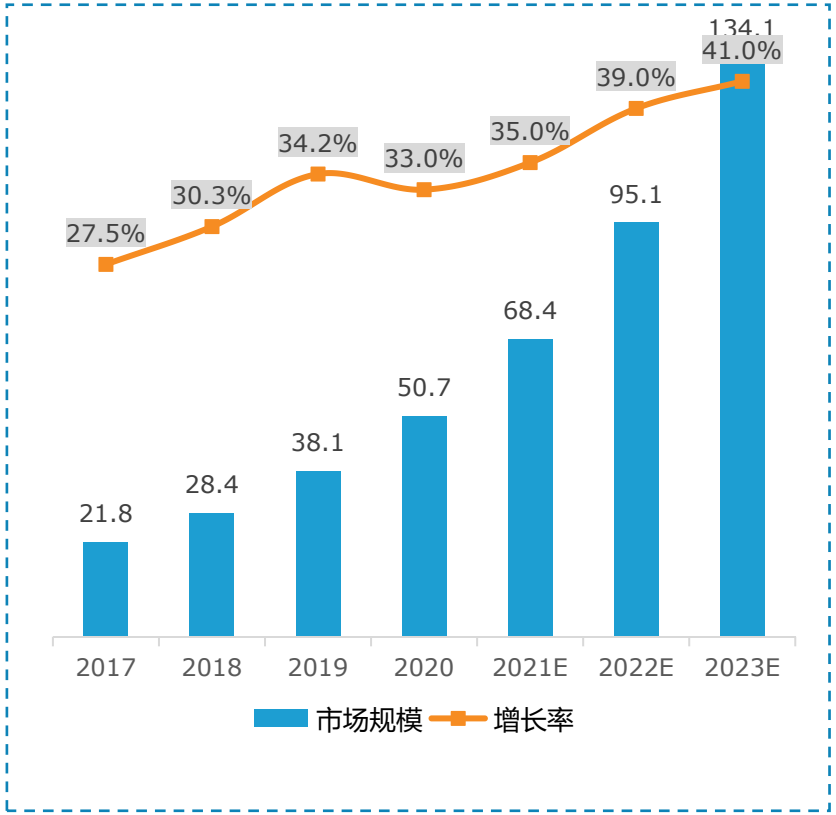
数字化网络安全正在成为网安市场发展的重要驱动力

◆随着信息产业不断升级，云计算、大数据、物联网与工业互联网不断渗透到各个行业。**相较于传统网络安全产品，行业细分领域如云安全、数据安全与物联网安全领域等需求正在超越传统安全产品赛道。**根据亿欧预测，2021年中国云安全、数据安全、物联网安全市场规模分别为113.1亿元、68.4亿元、 244.2亿元，2021-2023年各细分领域年均复合增速均超过 30.0%。

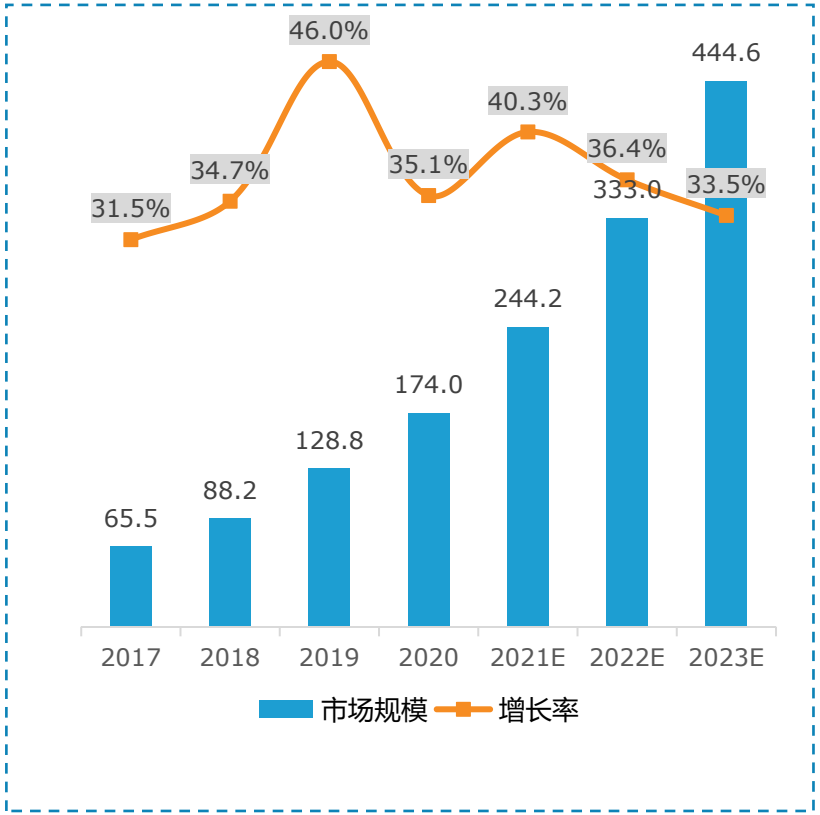
亿欧智库：2017-2023年中国云安全市场规模（单位：亿元人民币）



亿欧智库：2017-2023年中国数据安全市场规模（单位：亿元人民币）



亿欧智库：2017-2023年中国物联网安全市场规模（单位：亿元人民币）



来源：专家访谈、亿欧智库整理及测算

数字化网络安全发展形态

Development pattern of digital network security

云安全风险：云用户重点关注影响数据和业务的云安全问题

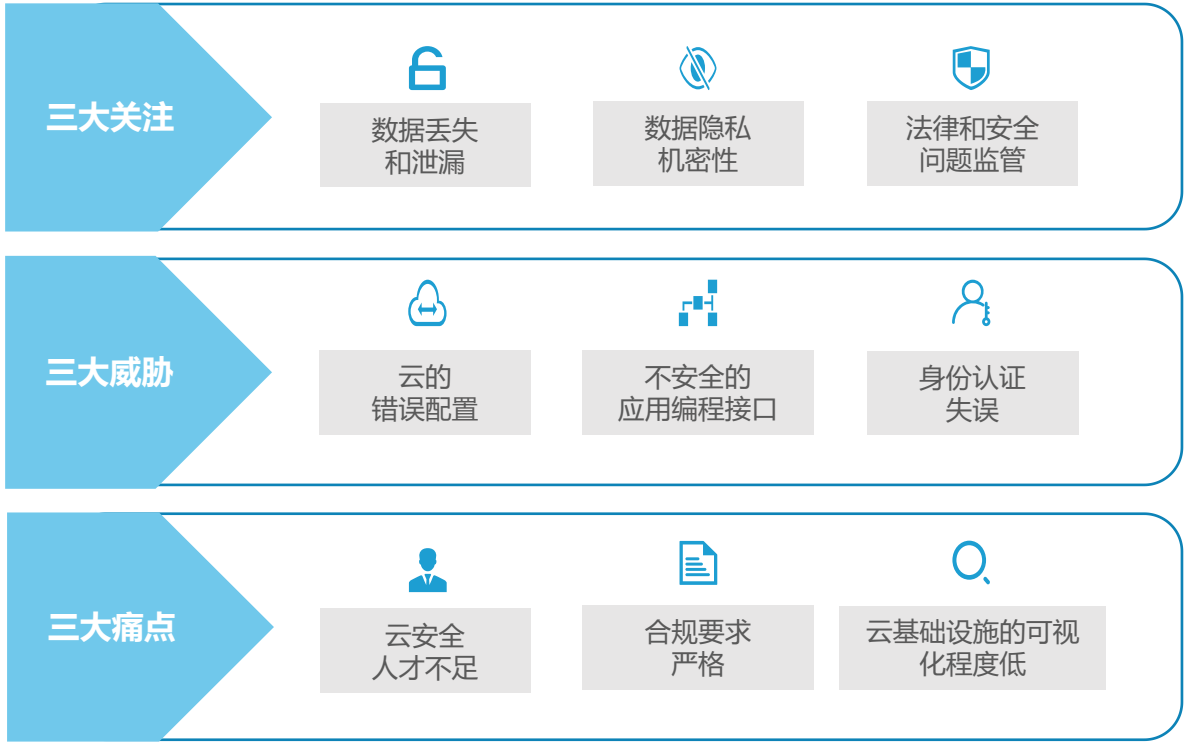
◆云计算承载着企业的数据及业务，因此用户一般关注对数据和业务会造成比较大影响的威胁。**尤其云数据中心数据、算力集中，诸如数据被勒索、数据丢失、数据泄露等安全威胁，成为了云上安全威胁的关注重点。**

◆2019年，云安全联盟（CSA）对行业专家进行了一次调查，根据调查问卷结果，行业专家最关切的12个云安全风险包括数据泄露、身份凭证和访问管理不足等。云计算专属安全问题主要集中在hypervisor层的安全威胁、虚拟资源的隔离机制变化和虚拟机的安全威胁等方面。

◆2020年，亚马逊（AWS）对427名云计算专家的调查显示了云用户对于云计算安全的关注点、威胁和痛点，**主要与数据、身份认证和合规相关。**

亿欧智库：CSA云安全联盟发布12大云安全风险

亿欧智库：2020年云用户关注点、面临的威胁以及痛点



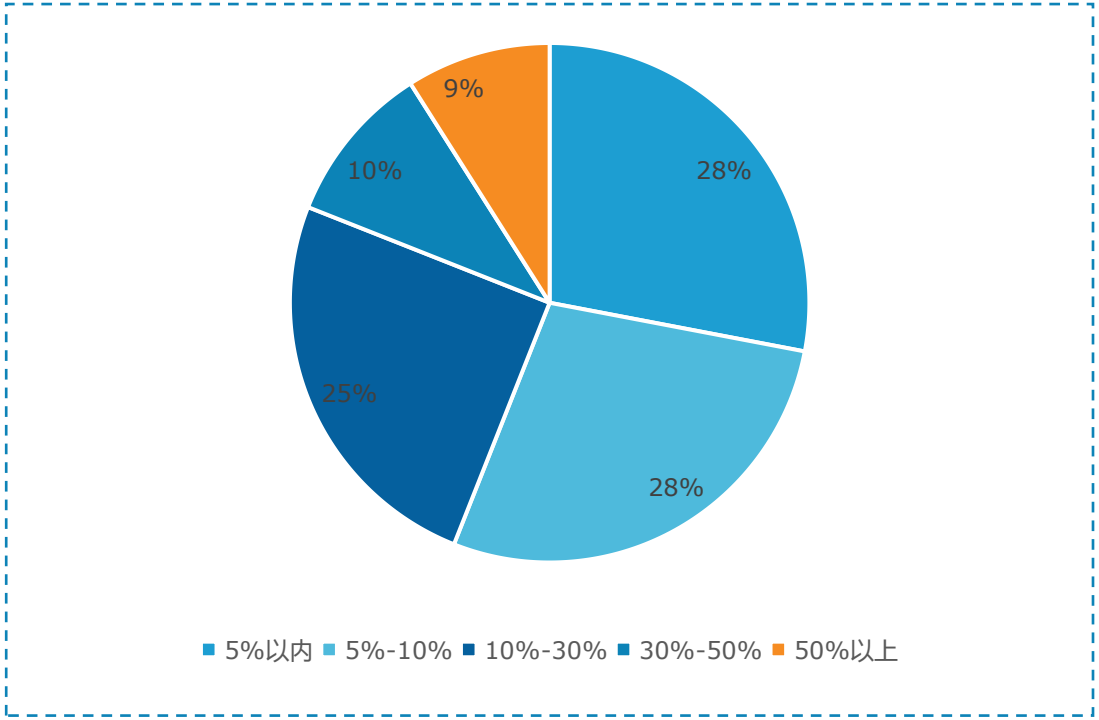
来源：云安全联盟、深信服、亚马逊

云安全风险：云原生改变IT底层架构，新的安全风险出现

◆云原生相对线下传统企业IT物理机上的环境，用云的方式来部署和管理应用，从而起到充分利用云效率的作用。云原生的全球渗透率不断提升，是云计算发展的大趋势。

◆根据云原生产业联盟发布的《中国云原生用户调查报告（2020）》，通过收集的487份调查问卷，现阶段已有9%的用户云原生相关投入占IT投入一半以上，云原生技术价值已经在用户侧得到初步认同。

亿欧智库：2020年云原生技术建设费用占总体IT投入的比例



亿欧智库： 云原生安全与传统安全的主要区别

	传统安全	云原生安全
安全模型	边界安全	端到端全链路安全
身份管理	基于IP地址	基于服务
隔离粒度	虚拟机或者物理机级别， 通过物理隔离或者管理程序实现隔离	容器级别的隔离
威胁应对	被动，快速检测威胁是首要任务 确定漏洞后才执行用以缓解威胁的步骤	云原生安全主动改变系统状态 破坏恶意软件的生产条件
漏洞修补	增量修补， 每个补丁程序都需要内部团队审批	通过重新部署进行修补， 带有全新组建的全新镜像应用到数据中心

来源：云原生产业联盟、亿欧智库整理

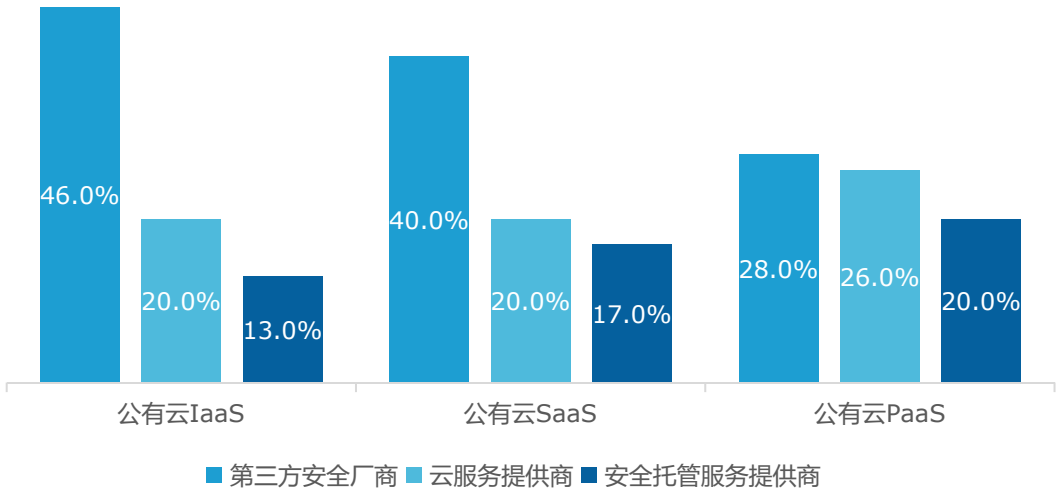
云安全防护：第三方提供的云安全产品是主流选择

◆云安全产品可以分为三类，**一类由云服务提供者直接提供，一类由第三方安全厂商提供，另外，第三方安全托管服务提供商也会提供云安全解决方案。**对于公有云来说，第三方安全厂商提供的产品最受欢迎。如果未来国内形成以私有云和混合云为主的趋势，第三方安全产品也将更有占据主流市场的潜力。

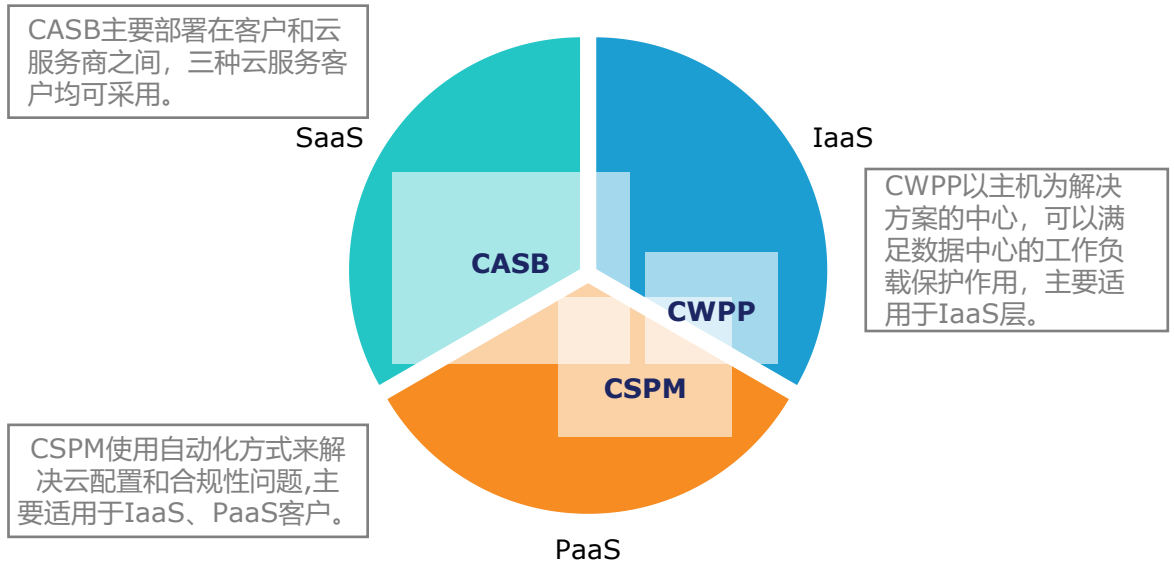
◆**云服务提供者（CSP）本身也是云安全产品的供应商。AWS、谷歌、阿里云都在推出自己的安全基础设施服务。**云服务提供商提供的安全产品通常包括威胁检测、云数据库安全、API安全、容器和工作负载安全、用户行为检测、合规与风险管理等。

◆第三方提供的安全产品主要负责保护用户侧的云安全，**主要的产品类型有CASB（云访问安全代理）、CWPP（云工作负载安全防护平台）、CSPM（云安全配置管理）等。**针对云原生安全也出现了SASE（安全访问服务边缘模型）技术以及有关集群、容器、微服务等安全措施。

亿欧智库：2019年公有云不同类型服务采用的安全产品比例



亿欧智库：第三方云产品CASB\CWPP\CSPM与三种类型云服务的关系



来源：青藤云安全 、开源证券

数据安全风险：数据泄漏事件占数据安全事件总体比重96.7%

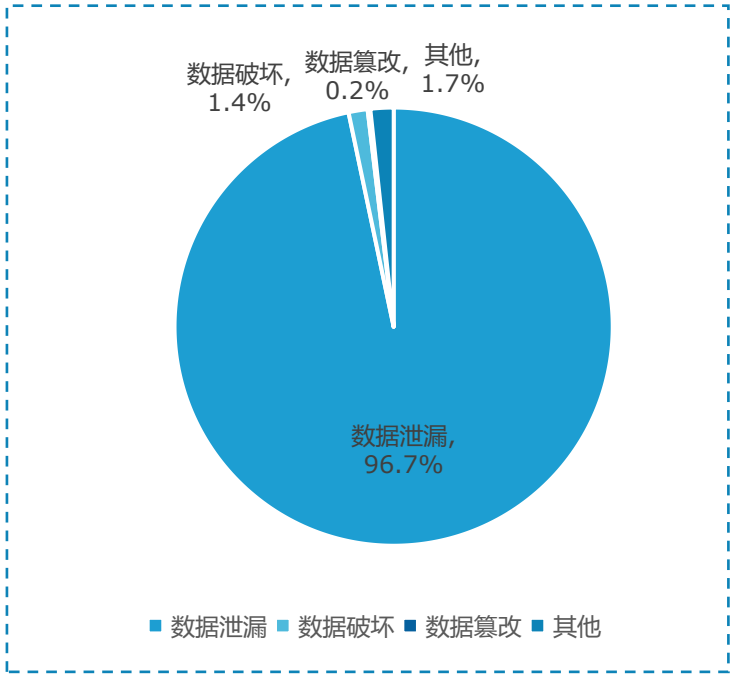
◆数据资源已经成为国家重要战略资源和新的生产要素，对经济发展、国家治理、社会管理、人民生活都产生了重大影响。数据安全指对数据在收集、存储、传输、处理、交换、销毁等活动中的保护，保障数据在全生命周期中，不被泄露、窃取、篡改、毁损、非法使用等，保证数据的完整性、保密性和可用性。

◆随着各行业对数据资源充分利用，2019年1月-2020年8月，安全内参共收录全球政企机构重大数据安全报道 420起，其中2019年286起，2020年1-8月134起；数据泄露相关安全事件高达406起，占总事件96.7%。在涉及数据安全事件的政企机构中，政府机构事业单位是应急响应处置的数据安全事件最多的领域，为169起，其次是医疗卫生行业，为118起。

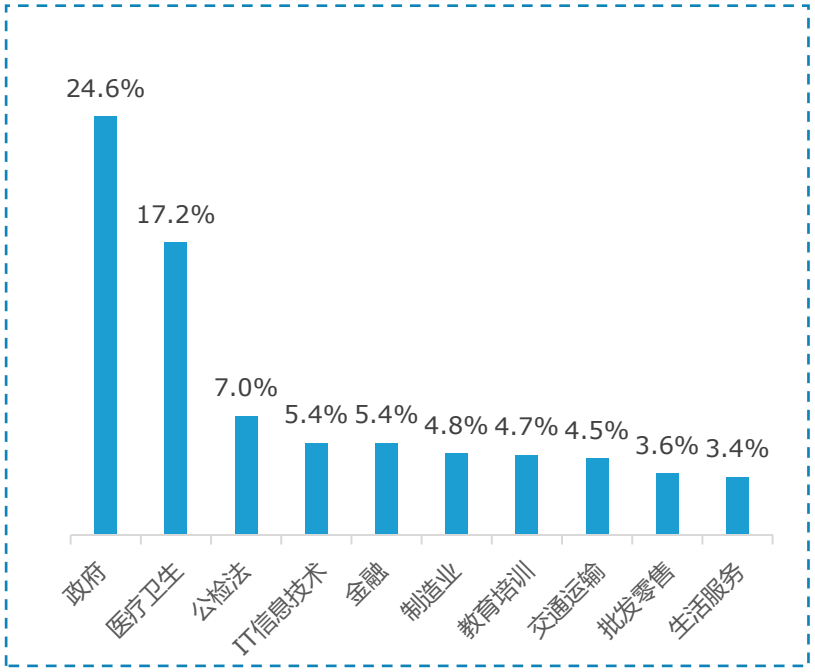
亿欧智库： 2019-2020年全球重大数据安全事件

时间	事件经过
2019年1月	爱尔兰有轨电车运营商网站被黑，黑客用乘客数据勒索 1 比特币
2019年11月	11.9亿份敏感医疗图像互联网暴露，包含美国军方人员信息
2019年11月	美国黑客组织攻击了全美110家养老院的计算机，并要求支付价值1400万美元的比特币才会解锁系统
2020年2月	拥有30亿人脸数据的美国AI公司Clearview AI 被黑
2020年1月	黑客破坏关联公司系统，入侵日本三菱公司网络基地
2020年2月	某SaaS服务商多家客户后台进入失败，订单无法处理，甚至服务商官方小程序也出现问题

亿欧智库：2019年1月-2020年8月全球数据安全事件类型分布



亿欧智库： 2019年1月-2020年8月全球政企机构数据安全应急事件行业分布



来源：安全内参、奇安信、亿欧智库整理

数据安全防护：覆盖数据全生命周期，搭建安全体系

◆在数字化时代，网络安全不再是传统IT基础设施的安全，还包括整个数字化生态中全部有形与无形的资产，尤其是数据资产。对数据的保护需要覆盖数据的全生命周期，亿欧智库引用国标GB/T37988-2019《信息安全技术 数据安全能力成熟度模型》DSMM架构图中的数据生存周期安全步骤，从数据采集、数据存储、数据传输、数据处理、数据交换、数据销毁六个阶段搭建安全体系。

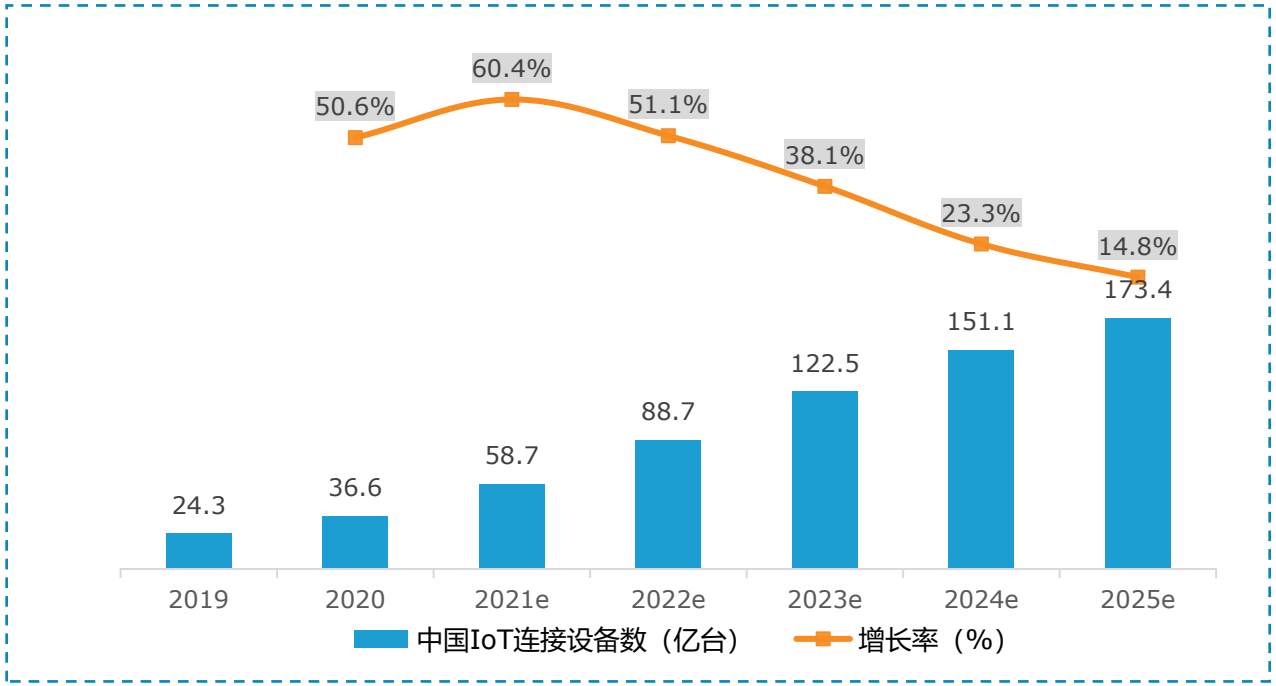
亿欧智库：数据安全防护体系

来源：《数据安全治理白皮书3.0（2021》、《绿盟数据安全白皮书2.0》

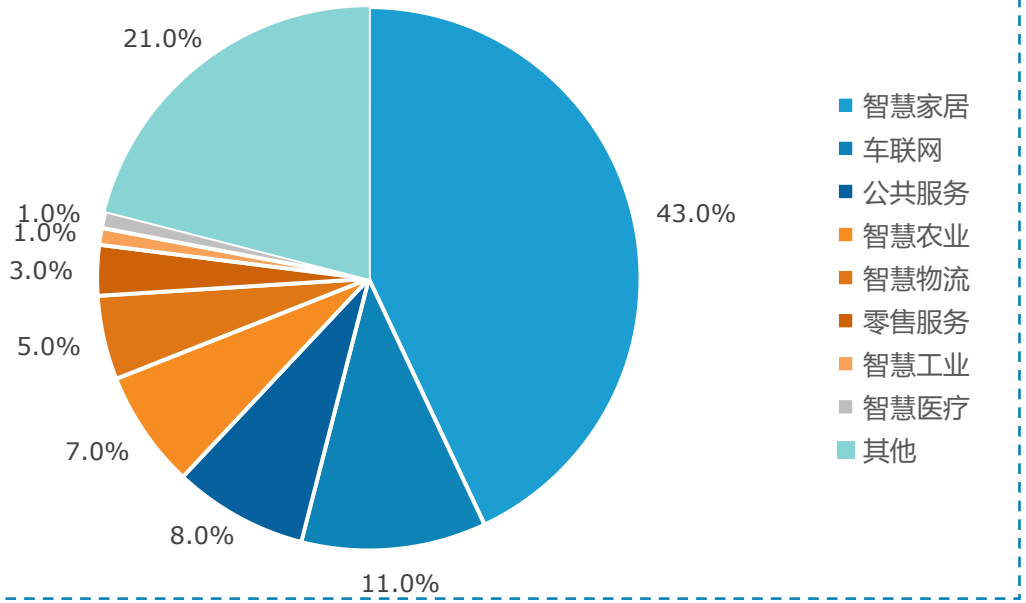
物联网安全风险： 2020年中国IoT连接设备数超30亿台，智慧家居、车联网成主要下游应用

◆随着车联网、智能家居、智能城市等物联网下游应用的普及，越来越多的连接设备进入到社会生活当中。2020年中国IoT连接设备数开始进入了规模化快速发展阶段。亿欧智库的数据显示，不包括手机、PC和笔记本电脑，2020年中国IoT连接设备数达到36.6亿台，相比2019年增长50.6%。接下来几年中国IoT连接设备数将保持高速增长态势；2021年，中国IoT连接设备数预计达58.7亿台。预计到2025年，这一数字将增长到173.4亿台，届时IoT将成为一个10倍于智能手机的大市场。

亿欧智库：2019-2025年中国IOT设备连接数
单位：亿台



亿欧智库：2020年物联网下游应用分布



来源： 兴业证券、亿欧智库测算

物联网安全风险：2021年3月物联网设备遭6亿次攻击，路由器、摄像头为重点攻击对象

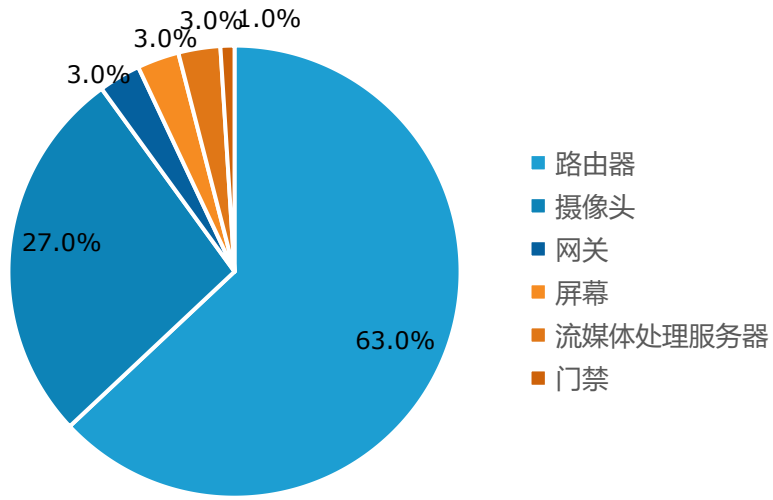
◆2020-2021年，物联网安全事件频发，穿戴设备、智能家居、安防摄像头、甚至市政公用设施和工业物联网设备遭受到攻击，影响恶劣。根据中国网信办下属的关键基础设施安全应急响应中心数据，自2021年3月1日至31日，共监测到物联网（IoT）设备攻击行为6亿余次，捕获IoT恶意样本2738个，发现IoT恶意程序传播IP地址21万余个、威胁资产（IP地址）155万余个，境内被攻击的设备地址达771万个。

◆为了解重点行业物联网网络安全态势，关键基础设施安全应急响应中心筛选了电力、石油、车联网和轨道交通等行业的2396个资产（含物联网设备及物联网相关的web资产）进行监测，结果显示，2021年4月，遭受攻击的资产有1355个，涉及攻击事件12454起。目前最容易受到攻击的物联网设备主要是路由器和摄像头设备。

亿欧智库： 2020年物联网重大安全事件

时间	事件经过
2020年1月	黑客泄露 51 万服务器路由器的 Telnet 密码
2020年2月	境外黑客组织发布推文扬言将于2月13日对中国视频监控系统实施网络攻击破坏活动
2020年7月	对华硕、AVM、D-Link、Linksys、Netgear、TP-Link和Zyxel等127个路由器模型进行的研究表明，没有一个路由器是没有已知漏洞的
2020年7月	以色列供水设施一个月内遭到两次网络攻击
2020年10月	圣路易斯的监狱视频探视供应商被发现存在一个安全漏洞，暴露了数千名囚犯和他们的家人之间的电话
2020年3月	攻击者通过攻击 D-Link 与 Linksys 路由器的方式，劫持用户的网络访问并重定向至伪造的新冠病毒主题页面，通过虚假告示信息诱骗用户下载恶意软件

亿欧智库：2020年物联网终端漏洞分布



来源：亿欧智库整理

物联网安全风险：感知层、网络层、平台层、应用层风险类型特征各异

◆物联网安全风险基于技术和应用架构产生。物联网的感知层由传感器、网关等设备组成，主要功能是实现对信息的采集、识别和控制，对终端加以安全防护是物联网业务安全的根源；网络层主要用于将感知层获取的信息进行传递和处理，由于物联网有很多非标准的传输协议，面临的网络安全威胁更为复杂；平台层具有数据收集处理、处理结果向用户界面接口反馈等基本功能，涉及多种安全风险；应用层也可能受到网络安全攻击，风险波及终端用户。

亿欧智库： 物联网感知层、网络层、平台层、应用层的不同风险

感知层	网络层	平台层	应用层
终端安全风险	网络安全风险	平台安全风险	应用安全风险
• 终端物理风险（偷盗、移动等） • 终端自身风险（终端自身存在漏洞） • 不完善的通信机制 • 数据泄露风险 • 恶意软件感染风险 • 服务中断风险	• 无线数据链路脆弱性 • 拒绝服务攻击（DDOS） • 非授权接入和访问网络 • 运营商应急管控风险	• 平台存储大量数据,易成为攻击焦点 • 虚拟化、容器技术带来新安全风险 • 平台基础环境漏洞存在风险	• 利用应用漏洞窃取用户文件隐私 • 传播僵尸程序劫持智能设备 • 通过控制设备反向攻击云平台 • 窃取破坏数据 • ……

来源：亿欧智库整理

物联网安全风险：防护难度大，物联网安全领域主要为三类厂商

◆中国有超过2500万家物联网终端设备生产商，终端安全防护能力参差不齐。物联网安全威胁与传统网络安全威胁相比，其扩散能力和规模潜力都更为突出。因此对于物联网安全攻防双方来讲，防守端难度更大，更具挑战。

◆物联网安全产品和服务的提供者主要为：1）综合类厂商，专门成立物联网安全部门；2）专注于物联网安全的专精型厂商；3）物联网产业链厂商通过新增事业部等方式进入物联网安全领域。

亿欧智库：物联网环境中的攻防双方优劣势对比

攻击者的优势	物联网设备特性	防守者的挑战
收益高、效果显著	设备基数规模大	防守成本高
攻击技术门槛低	安全设施薄弱	漏洞多且不易排查
多路玩家参与	设备种类多	技术复杂、技能线长
策划攻击性价比高	低成本设备多	安全投入性价比低
……	……	……

亿欧智库：物联网安全厂商分类

综合类安全厂商

专精型安全厂商

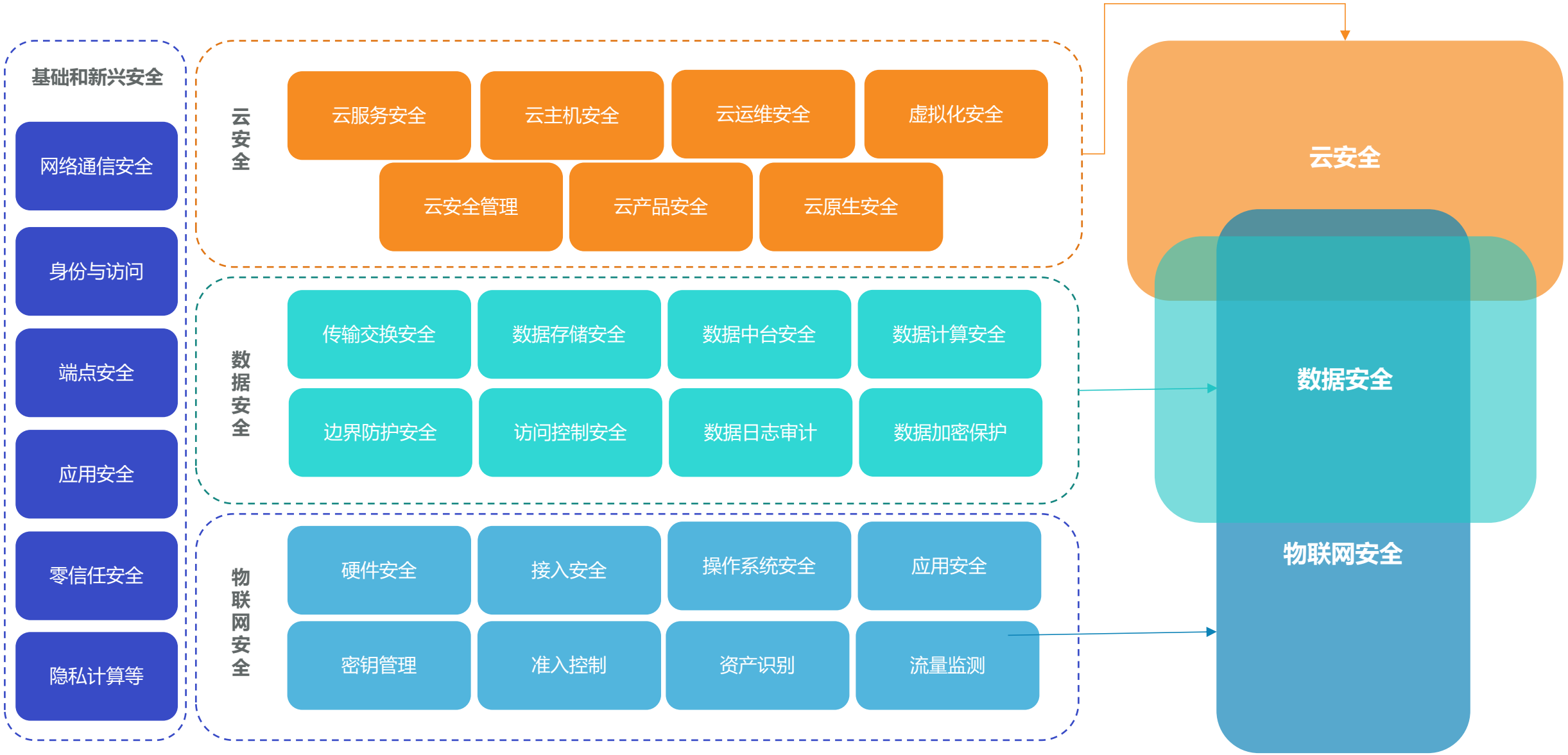
物联网产业链厂商

来源：亿欧智库整理

数字化网络安全技术框架

亿欧智库

亿欧智库：数字化网络安全技术框架



来源：亿欧智库整理

网络安全技术框架——云安全技术框架

◆由于云服务的特殊性，云安全需要云厂商和用户协助保证。云厂商主要负责云平台系统自身的安全，云用户主要负责云主机安全、云应用安全、云产品安全和云上数据安全。另外，云安全管理涵盖对整个平台体系的集中管控，是云安全建设的根本；云原生安全是云架构下一步发展方向提出的新的安全需求。

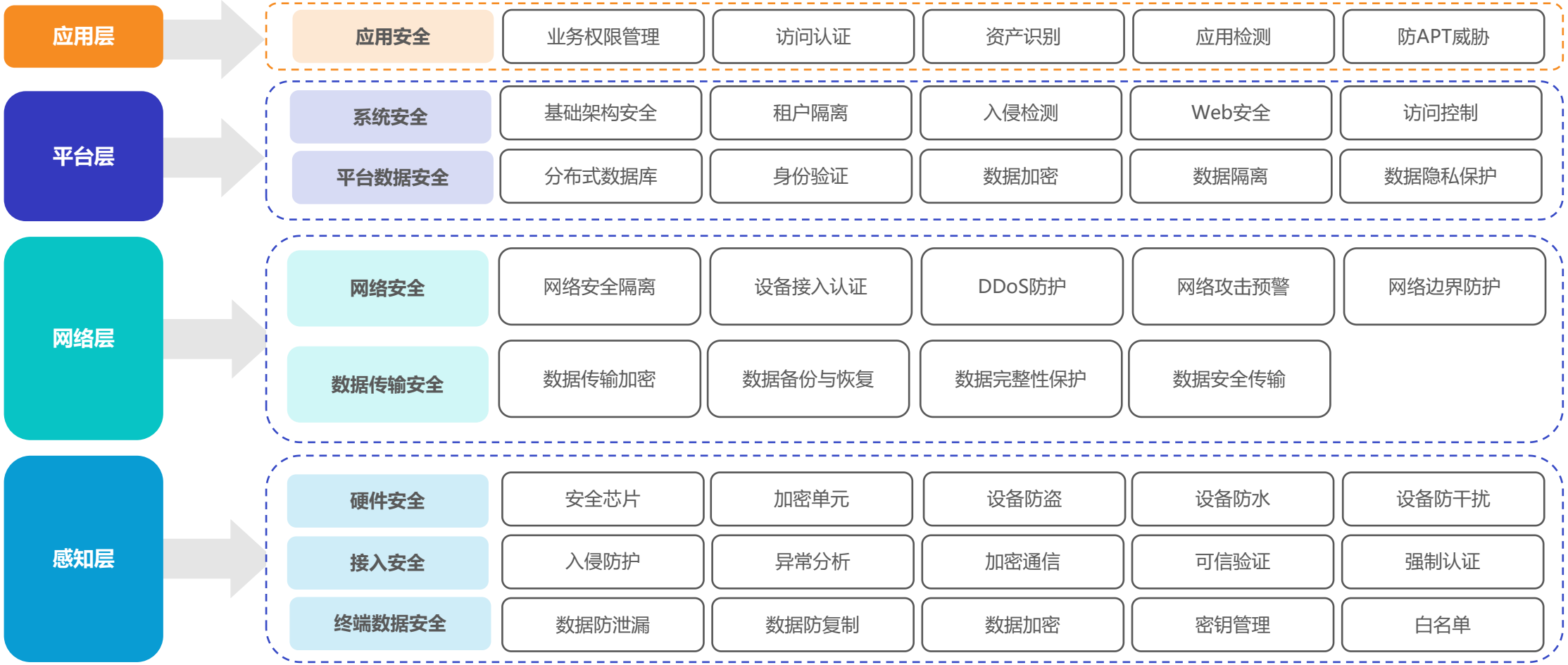
亿欧智库：云安全技术框架

来源：亿欧智库整理

网络安全技术框架——物联网安全技术框架

◆物联网安全的技术层次可以分为三个层面，感知层、网络层、平台和应用层。感知层安全主要包括设备安全、数据安全和网关接入安全；网络层安全主要指物联网终端网关到物联网后台处理平台之间的安全；平台和应用层安全主要指的是物联网后台数据处理平台和前台展示呈现的应用安全。以层次化进行物联网安全分析和防护是物联网安全体系的重要思路。

亿欧智库：物联网安全技术框架



来源：亿欧智库整理

网络安全技术框架——数据安全技术框架

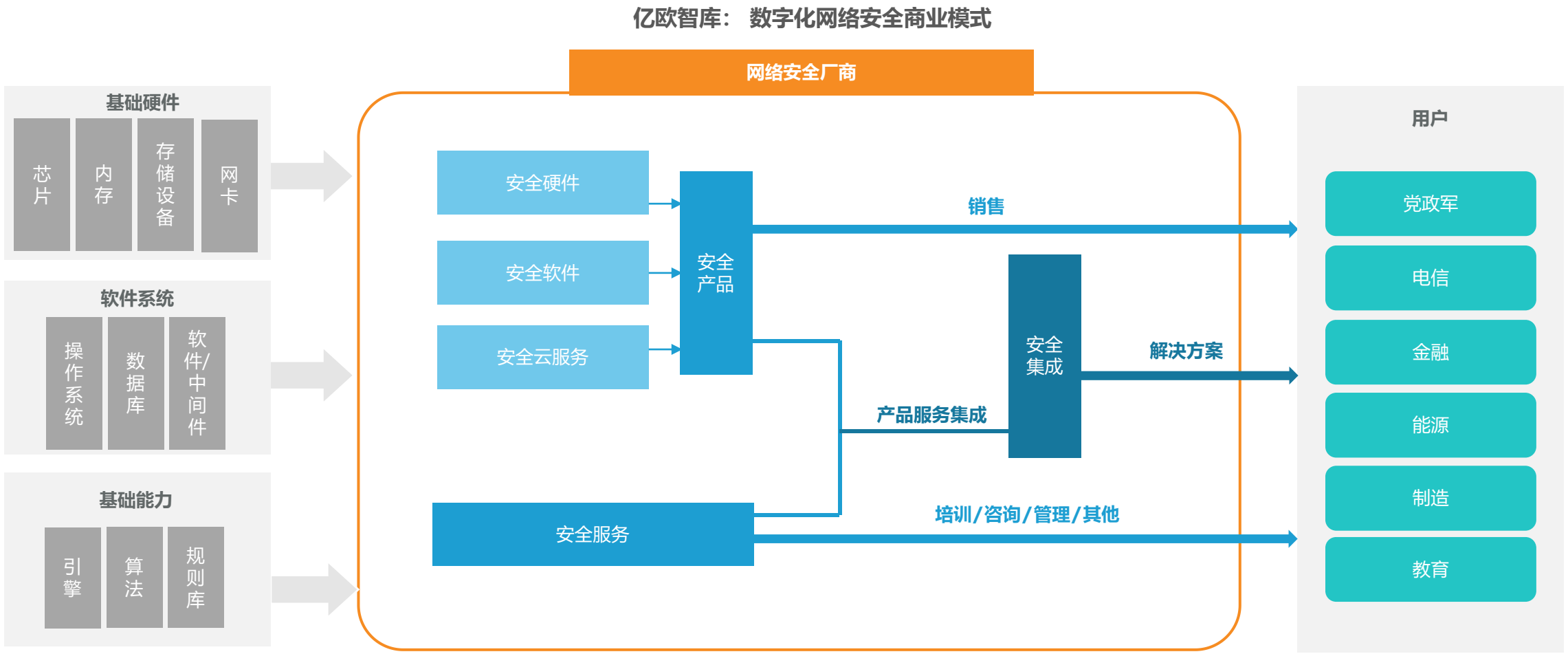
◆按照数据生命周期，遵循“事前客观、事中可控、事后可追溯”的原则，可以将数据安全框架分为数据采集安全、数据传输安全、数据存储安全、数据处理安全和数据销毁安全六大步骤，以及风险与需求识别、风险防护、追溯恢复三大模块。

亿欧智库： 数据安全技术框架

风险识别	数据资产梳理	数据资产分级	敏感数据标记	数据暴露面识别	防护需求识别	身份权限体系	事前
风险防护	数据采集安全	数据传输安全	数据存储安全	数据处理安全		数据销毁安全	事中
	数据采集合规	传输加密	合理存储位置	身份及访问管理	处理权限控制	数据有效期策略	
	最小化采集策略	传输身份认证	敏感数据隔离	用户实体行为分析	数据显示限制		
	采集风险评估	跨境传输监测	数据存储加密	特殊行为监测	访问设备限制	存储介质销毁	
	授权明示同意	数据完整性验证	存储时间限制	数字水印	数据暴露面监测		
	其他隐私政策	数据外发控制	数据脱敏存储	可信认证	安全合规监测	敏感数据销毁	
追溯与恢复	数据流向回溯	事件溯源	行为审计	日志审核	数据灾备	数据备份与恢复	事后

来源：亿欧智库整理

数字化网络安全商业模式：网络安全厂商以提供产品和服务为主

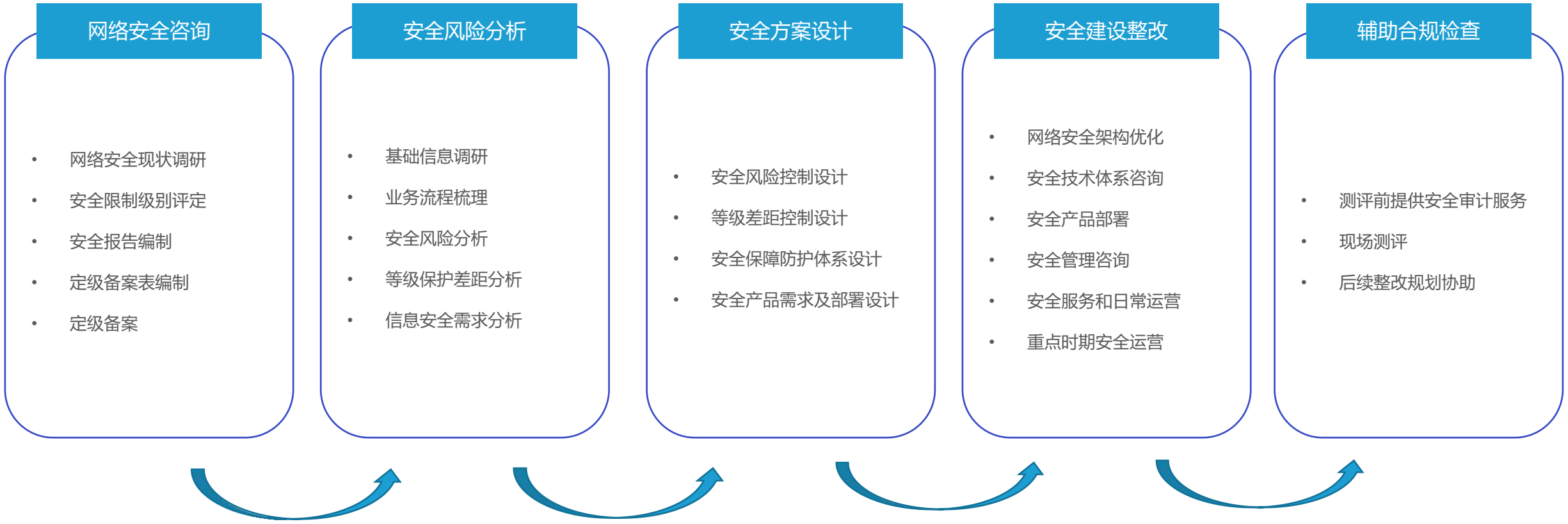


来源：专家访谈、亿欧智库整理

数字化网络安全商业模式：安全集成服务正在成为网安需求热点

◆随着新基建陆续展开，移动互联网、工业互联网的快速发展极大拓展了网络攻击的渠道，攻击模式急剧多元复杂化，客户对网安厂商全面防御的要求提升。同时，随着物联网、工业互联网、云计算、大数据等新兴技术的兴起，网络攻击形态日益复杂，单一领域的单一产品无法再满足网络安全防护需求，安全集成服务正逐步成为网安需求热点。

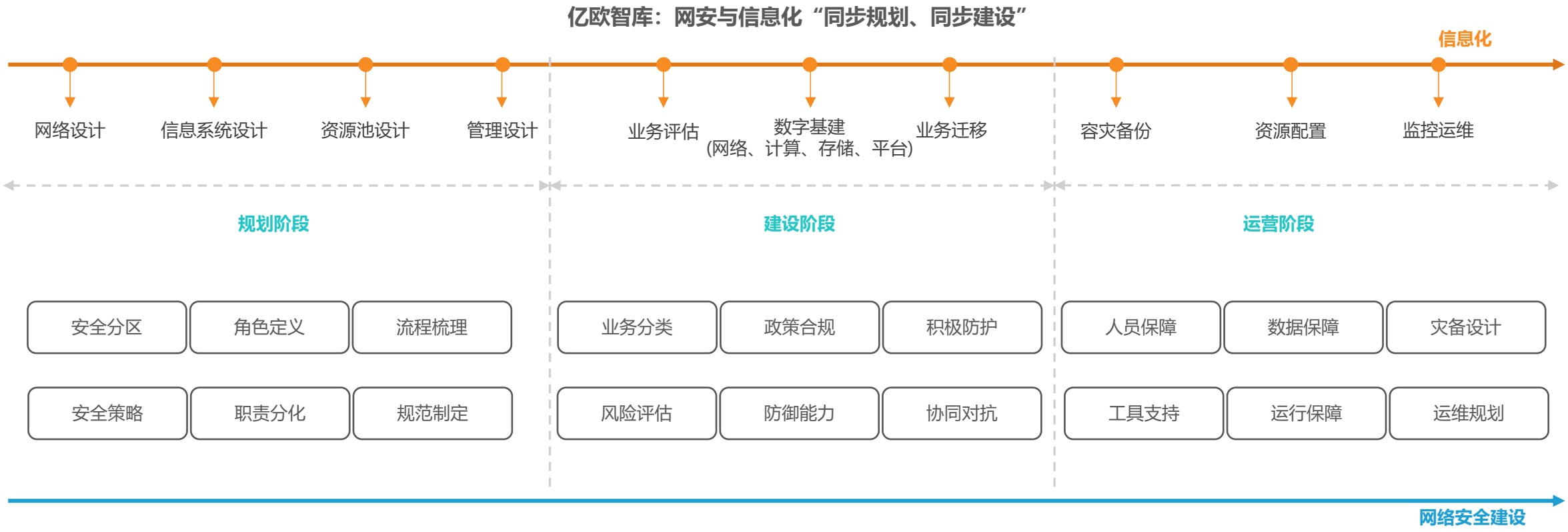
亿欧智库：等级保护集成安全服务模式



来源：亿欧智库整理

数字化网络安全商业模式：网络安全应与信息化“同步规划、同步建设”

◆从行业发展来看，网络安全发展一直落后于信息化的发展。脱节的原因不仅仅在于技术层，更在于体系化、战略上对网络安全的不够重视。虽然不少企业开始同步执行业务战略与信息化战略，但网络安全并没有跟上前两者的发展脚步。因此，当前网络安全能力和水平不能充分满足政企信息化发展的需要。《网络安全法》中已明确提出，网络安全要和信息化同步规划、同步建设和同步运营。



来源：亿欧智库整理

数字化网络安全产业图谱

亿欧智库

上游

基础硬件

芯片：infineon、HISILICON、LOONGSON龙芯、飞腾 PHYTIUM、intel

内存：ADATA 威刚科技、SAMSUNG、CORSAIR、G.SKILL、Kingston、HUAWEI

存储设备：中科曙光 sinodata、ECCOii 华讯网络、紫光华智、smartx、inspur 浪潮

网卡：HUAWEI、D-Link、tp-link、intel

软件系统

操作系统：ThunderSoft 中科创达、诚迈科技 ARCHERMIND、统信软件 UNIONTECH、中科曙光 Sugon、中标软件

数据库：瀚高 HIGH GO、优炫软件 UXSINO、人大金仓 Kingbase、神舟通用、达梦数据库、GBASE 南大通用

软件：Kingdee 金蝶、普元 PRIMETON、东方通 TongTech、HUAWEI、统信软件 UNIONTECH、KYLINSOFT 麒麟软件

基础能力

引擎：H3C 数字化解决方案领导者、inspur 浪潮、蚂蚁金服 ANT FINANCIAL、中科曙光 Sugon、TRANSWARP 星环科技

算法：云图 YUNTOP.COM、Cambricon 寒武纪、商汤 sensetime、LEVZ TECH、云知声

中游

综合类企业

奇安信、Venus、启明星辰、SANGFOR 深信服科技、NSFOCUS 绿盟科技、AsiaInfo、亚信安全、Westone·卫士通、H3C 数字化解决方案领导者、Hillstone 山石网科、DBAPP Security 安恒信息、ZTE中兴

身份安全

竹云 bamboocloud、AsiaInfo 亚信安全、芯盾时代 TRUSFORT.COM、齐治科技、派拉软件 PARAVIEW SOFTWARE、安讯奔、玉符科技 YUFU Identity、海颐软件 HAIYI SOFTWARE、格尔软件 KOAL、数字认证

端点安全

联软科技、Infogo 盈高科技、北信源 VRV、安天、安芯网盾、猎鹰安全 Falcon Security、火绒安全 www.huorong.cn、GSC 通软、杰思安全

应用安全

开源网安 SECZONE GROUP、保时达 Keep Danger Away、邦盛科技 Bangsun Technology、昂楷 ANMINOR、同盾科技 www.tongdun.cn、瑞数信息 RIVER SECURITY、默安科技、思维达纪

边界安全

H3C 数字化解决方案领导者、Hillstone 山石网科、NSFOCUS 绿盟科技、伟思信安 victory·idea、TIPTOP利普、天行网安 TOPWALK、奇安信、SANGFOR 深信服科技、中睿天下

安全运维及服务

火线、华清信安、GooAnn、安天、国舜、魔方安全 CUBESEC TECH、ALLSEC、观安

云安全

杰思安全、知道创宇、Vesystem、默安科技、网宿科技 ChinaNetCenter、华数网络、SkyGuard、国云科技、阿里云、安全狗、长亭科技 CHAITIN、QINGTENG 青藤云安全、易安联、SUNYAINFO、clerware、白山云科技 BAISHANCLOUD、腾讯云

数据安全

SkyGuard、中安威士 VISUALSEC、中孚信息、连山科技 LSSEC TECH、志翔科技、明朗万达 Wondersoft、ESAFENET 亿赛通、DBSEC、SUNINFO、时代亿信、Vamtoo 华途、ANKKI、昂楷科技、思维达纪、微智信业 MICROVISION、sansec 三未信安、观安、SCUTECH 鼎甲科技

物联网安全

Neusoft东软、信大捷安、慧盾安全 SmartSec、纬德信息 WEIDENG、uniview 宇视科技、天防安全 Tianfang Sec、青莲云、云盾、天行网安 TOPWALK、信长城、梆梆安全 BANGCLE、SPEED TECHNOLOGY、Bingsoft

工控安全

立思辰 LANXUM、威努特 WINICSSEC、安帝科技 ANDISEC、长扬科技 CHANGYANG TECH、安盟信息 SECURITYUNION、6cloud 六方云 让|万|物|安|全|互|联、烽台科技 FENGTAI TECHNOLOGY、圣博润 SBR-info、天地和兴 TIANDI HEXING

移动安全

梆梆安全 BANGCLE、nesun 能信安、海云安 secoder、指掌易、通付盾 Pay Egis、筑泰防务、启迪国信、芯盾时代 TRUSFORT.COM、北卡科技 BEIKATECH

下游

党政军

电信运营商

中国移动 China Mobile、China unicom中国联通、中国电信 CHINA TELECOM

能源企业

国家电网 STATE GRID CORPORATION OF CHINA、中国石油、中国石化 SINOPEC、中国南方电网 CHINA SOUTHERN POWER GRID

工业企业

中国航天 CASC、中国电科 CETC、长城汽车 Great Wall、中国铁建 CRCC

金融企业

中国银行 BANK OF CHINA、中信证券 CITIC SECURITIES、中国人寿 CHINA LIFE、博时基金

教育医疗

南京大学、浙江大学、复旦大学、上海交通大学

机遇与挑战

Opportunities and Challenges

新技术发展机遇：零信任——永不信任、持续验证

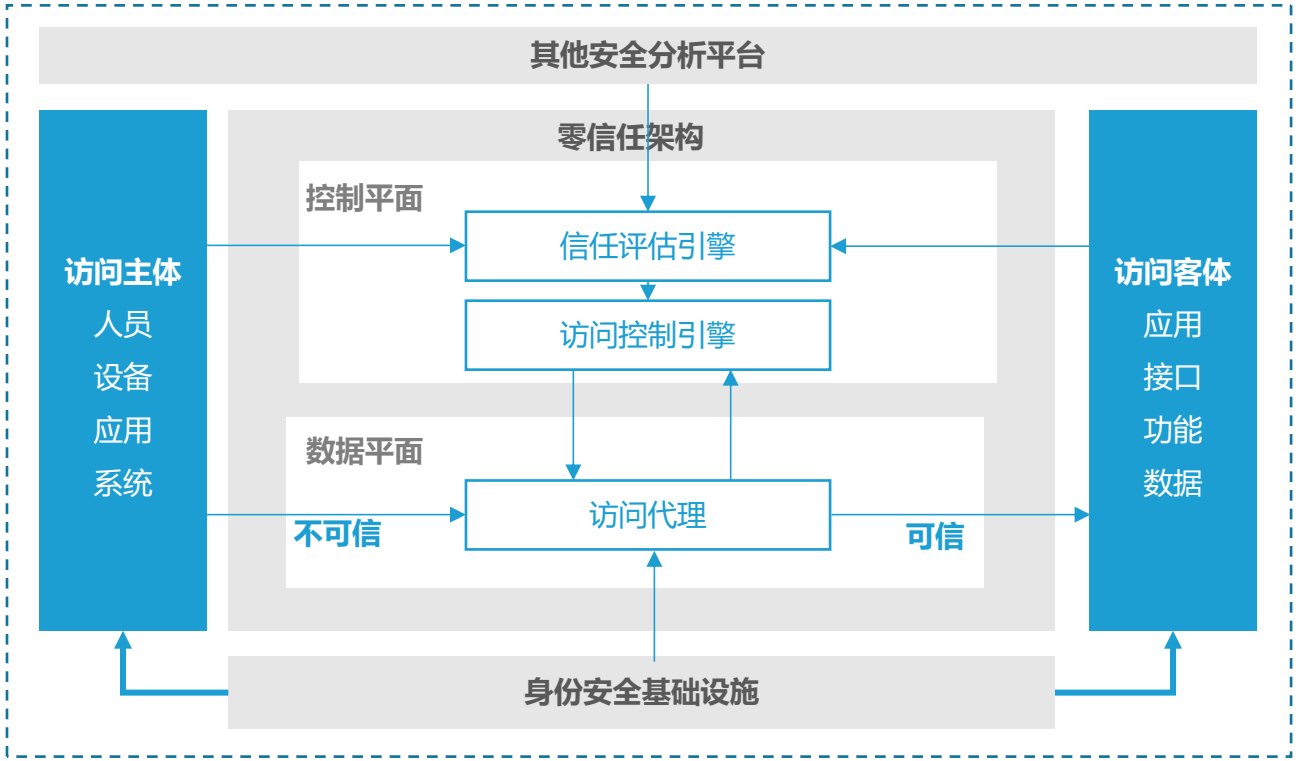
◆随着数字化转型的逐步深入，以及疫情影响带来的远程工作趋势，使得政企内部网络的物理边界正在被不断的淡化瓦解，传统的边界防护不再能够实现有效的安全保障，新的网络安全架构亟需建立。此时，零信任安全架构凭借其创新性的解决方式赢得了人们的关注。

◆零信任的核心安全理念是“永不信任、持续验证”，即：默认情况下，组织内外部的任何人、事、物均不可信，应在授权前对任何试图接入和访问网络的人、事、物进行验证。零信任基本原则可以归纳为：1）默认一切对象皆不可信；2）仅授予行为所需的最小权限；3）动态访问控制及授权；4）持续安全防护。

亿欧智库：零信任安全架构与传统安全架构的比较

	传统安全架构	零信任安全架构
防护对象	以“网络”为中心的防护	以“数据”为中心的防护
	以“攻防对抗”为主	关注“应用、资源”
防护基础	基于“边界”的防护	“无边界”防护
	以“信任”为基础	默认“不信任”，最小权限
防护理念	一次认证、静态策略	持续评估、动态访问控制
	被动、静态的防御	主动、自动化防御
信任范围	边界防护	无边界防护
	网络边界内部可信任	边界内外部均不可信任

亿欧智库：零信任技术架构图



来源：亿欧智库整理

新技术发展机遇：云原生安全——防护新的IT基础设施架构

◆云计算是信息技术发展和服务模式创新的集中体现，是信息化发展的重要变革和必然趋势。云原生技术架构充分利用了云计算弹性、敏捷、资源池和服务化特性，在改变云端应用的设计、开发、部署和运行模式的同时，也带来了新的安全需求和挑战。传统基于边界的防护模型已不能完全满足云原生的安全需求，全新的云原生安全防护模式应运而生。

◆云原生带来安全隐患的主要原因有：1）服务实例应用周期变短增加监控和溯源难度；2）组件爆发式增长为应用防护能力提出更高要求；3）容器共享操作系统的进程级隔离环境增加逃逸风险；4）独立研发运营对软件流转的全链条安全提出新要求。

亿欧智库：云原生安全风险类型

计算环境风险	微服务风险	Serverless风险	DevOps风险	API风险
云原生网络安全风险	攻击端口和攻击面增加	应用程序固有风险	设计风险：安全理念不足	未授权访问
云原生编排及组件安全风险	访问控制风险	Serverless计算模型风险	流程风险：安全流程缺失	数据泄露
镜像安全风险	治理框架风险	Serverless平台风险	管理风险：人员权限过大	DDOS风险
镜像仓库安全风险			开源风险：开源工具使用	
容器逃逸风险				

亿欧智库：云原生安全防护模型架构图

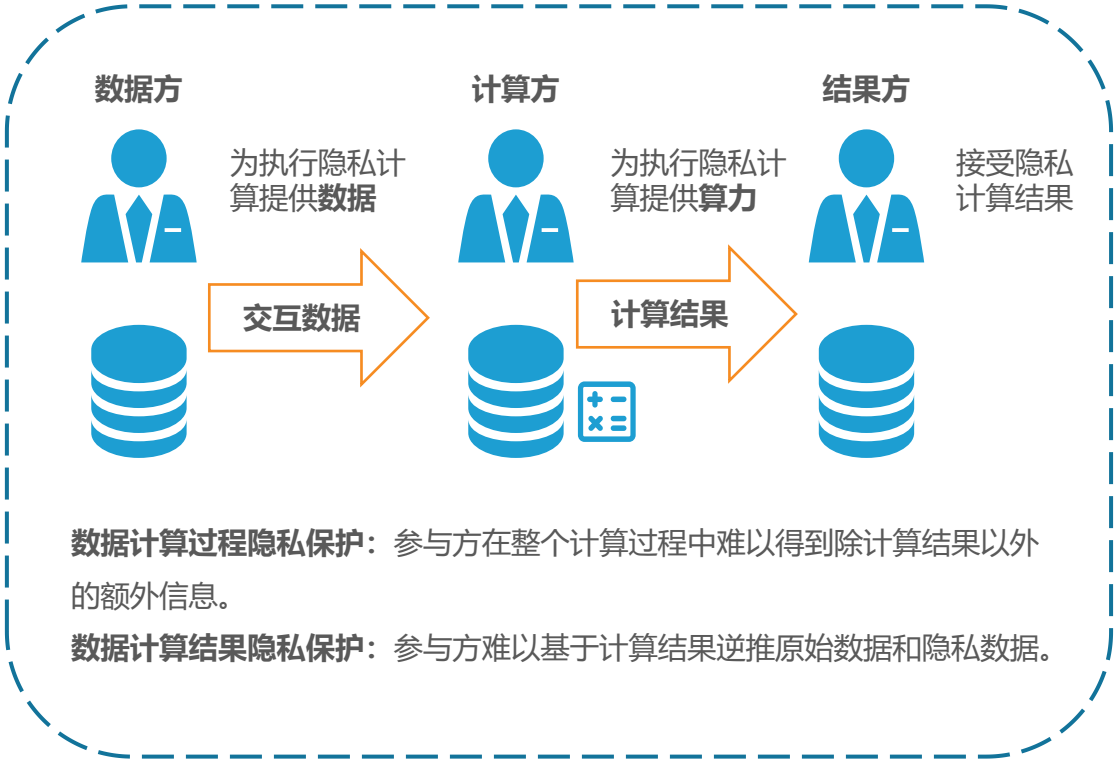
来源：中国信通院、专家访谈，亿欧智库整理

新技术发展机遇：隐私计算——帮助数据安全流通和使用

◆数据在推动数字经济不断发展进步的同时，数据的安全合规也日益成为人们关注的焦点。隐私计算技术的兴起，为人们提供了在数据安全合规和融合应用过程中寻求发展和安全之间平衡点的技术路径和解决思路，正成为未来数字治理的有效路径之一。

◆隐私计算（Privacy Computing）是一种由两个或多个参与方联合计算的技术和系统，参与方在不泄露各自数据的前提下通过协作对他们的数据进行联合机器学习和联合分析，其中联邦学习、多方安全计算和可信计算是当前主流技术路径，也是当下产品化的主要方向。

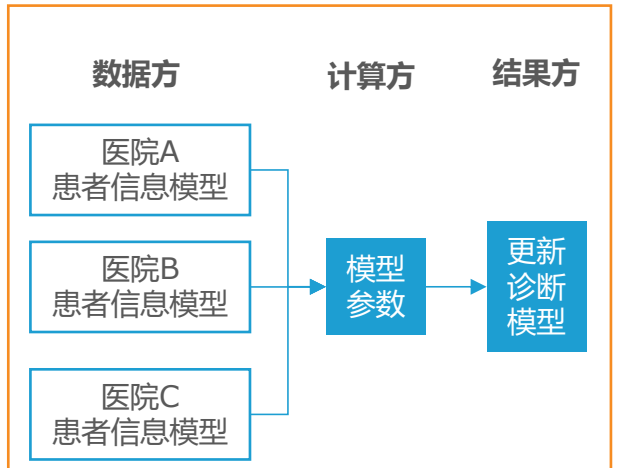
亿欧智库：隐私保护计算架构



数据计算过程隐私保护：参与方在整个计算过程中难以得到除计算结果以外的额外信息。

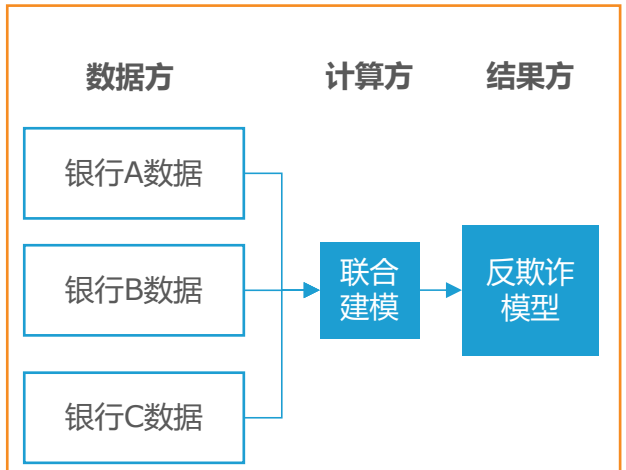
数据计算结果隐私保护：参与方难以基于计算结果逆推原始数据和隐私数据。

亿欧智库：隐私计算应用



医疗诊断隐私计算应用：

各医疗机构先在本地建立患者模型，再通过多方计算技术更新模型参数，在保障患者隐私的前提下提升诊断的准确性。



金融隐私计算应用：

多家金融机构联合建模，当一家银行获取新型欺诈行为数据时，实时更新反欺诈模型，提高整个金融系统的反欺诈能力。

来源：专家访谈，亿欧智库整理

市场机遇：网络安全投资聚焦数据安全、零信任、工控安全

◆2020年网络安全领域融资企业共30余家，主要聚焦领域为**数据安全、零信任、工控安全**等，融资轮次主要集中B轮，融资金额在数千万至几亿不等。据Canalys最新报告预测，与2020年相比，乐观估计2021年全球网络安全投资将增长约10%。

亿欧智库：2020年中国网络安全领域投资汇总

公司	轮次	金额	主要聚焦领域	公司	轮次	金额	主要聚焦领域	公司	轮次	金额	主要聚焦领域
天空卫士	B+	1亿人民币	数据安全	悬镜安全	Pre-A轮	数千万人民币	DevSecOps	数盾信息	C轮	1亿人民币	密码安全
青藤云	B+轮	3亿人民币	云安全	虎符网络	天使轮	近千万人民币	零信任	融安网络	B轮	近亿人民币	工控安全
蒸汽记忆	天使轮	数千万人民币	身份认证	齐治科技	战略投资	数亿人民币	数据安全	竹云科技	战略投资	3亿人民币	身份认证
斗象科技	C轮	数亿人民币	漏洞检测	瑞数信息	C＋轮	1.3亿人民币	数据安全	博智安全	D轮	3.7亿人民币	工控安全
易安联	B轮	近亿人民币	零信任	亚信安全	战略投资	未透露	数据安全	绎云科技	天使轮	千万级人民币	零信任
中科金审	B轮	未透露	数据安全	深信科创	天使轮	千万级人民币	人工智能安全	云天安全	Pre-A轮	6000万人民币	工控安全
联软科技	B轮	近亿人民币	端点安全	长扬科技	C轮	1.5亿人民币	工业互联网安全	北方实验室	战略投资	未透露	网络安全服务
赛宁网安	Pre-B轮	未透露	攻防安全	默安科技	B轮	3000万人民币	云安全	微步在线	D轮	3亿人民币	接入安全
万里红	战略投资	3亿人民币	信息保密安全	赋乐科技	B轮	数千万人民币	数据安全	中睿天下	B轮	近亿人民币	Web安全
六方云	B＋轮	数千万人民币	工业互联网安全	珞安科技	B轮	数千万人民币	工业安全	码牛科技	B轮	1亿人民币	信息安全
源堡科技	A轮	数千万人民币	风险管理	零时科技	天使轮	数百万人民币	区块链安全				

来源：亿欧智库整理

市场机遇：等保2.0、信创成为未来3-5年网络安全行业发展重要驱动力

◆2019年公安部发布网络安全等级保护2.0版本，正式宣告进入等保2.0时代。为了符合等保2.0的规范和要求，拥有第三级及以上信息系统较多的政府、金融、电信等领域将加大软硬件产品的投入，未来几年，等保2.0将成为网络安全行业最重要的驱动力之一。

◆信创产业主要由基础硬件、基础软件、应用软件、信息安全四部分构成，2020年是信创产业全面推广的起点，信创产业蓬勃发展，需要安全服务为其保驾护航。针对信创安全，各厂商已经逐步推进终端安全、安全测试、漏洞管理、安全开发等工作。

亿欧智库：2020年等保2.0潜在新增市场空间测算

行业		2020E市场规模（亿元）	安全支出占IT支出比例	等保增量市场规模（亿元）
新兴市场	云计算	1366	1.84%	25.1
	物联网	17211		316.7
	工业互联网	9329		171.7
	大数据	578		10.6
传统市场	政府、金融等典型各行业客户为主	24672	0.16%	39.5
合计市场空间				563.6

亿欧智库：信创产业全景图

来源：专家访谈、华西证券研究所、亿欧智库整理

市场机遇：AI发展带来网络安全需求，同时助力安全技术升级

◆人工智能技术发展对于网络安全是把双刃剑，攻击者可以通过AI来改善攻击方案，防守者可以充分利用AI技术，发现安全威胁，用AI对抗AI。总体来看，网络安全防护需要保护AI驱动的系统，并且预测攻击者对AI的使用；在威胁检测、模式识别和缩短响应时间方面，防守者通过AI技术分析大量数据，加强安全防御能力。

◆根据市场调研机构Meticulous Research的最新报告，预计网络安全市场中的人工智能市场规模从2020年开始将以23.6%的复合年增长率增长，到2027年将达到463亿美元。

亿欧智库：人工智能在网络安全领域的实现模式

亿欧智库：AI技术在网络安全领域的应用

人工智能技术	应用
机器学习（ML）	增强系统的预测能力，动态防御攻击，提升安全事件响应能力
专家系统（ES）	用于安全事件发生时为人提供决策辅助或部分自主决策
过程自动化（AT）	代替或协助人类进行检测或修复，尤其是安全事件的审计、取证
深度学习（DL）	探测与防御、威胁情报感知
自然语言处理（NLP）	可用于理解文字、语音等人类创造的内容，在内容安全领域不可或缺
图像处理（IP）	对图像进行分析，处理不良信息

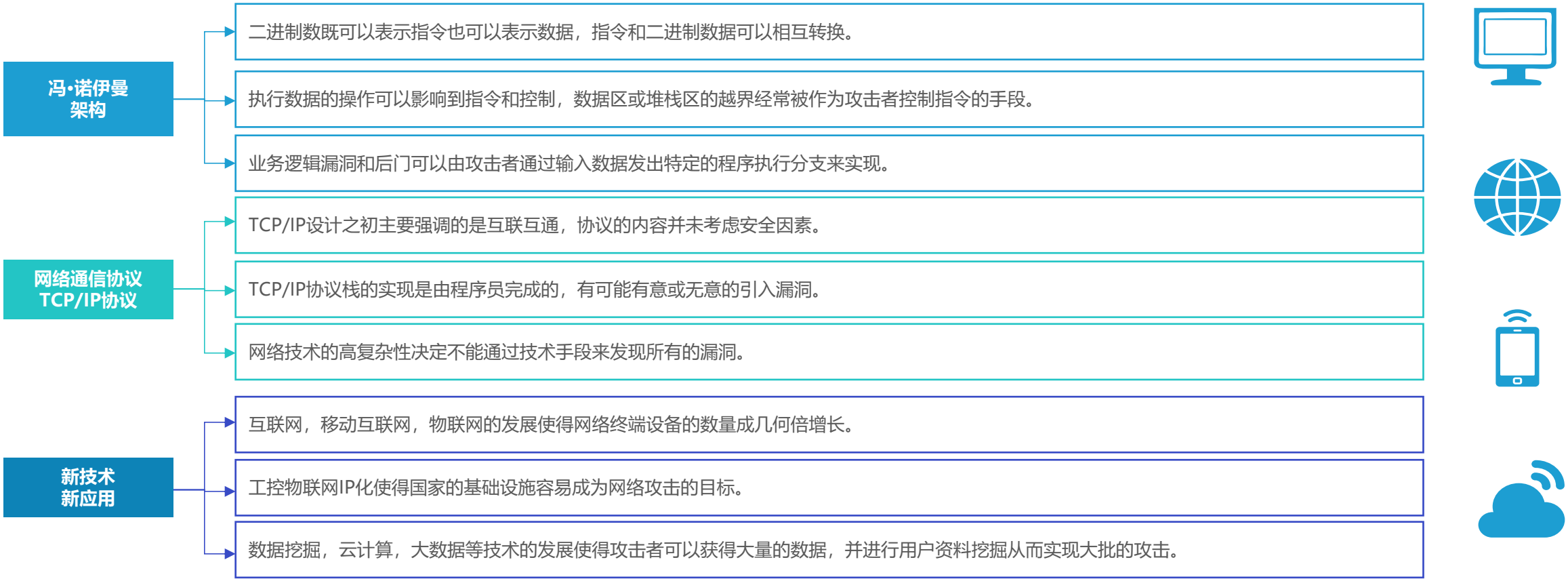
人工智能技术	应用
视频分析技术（VA）	识别视频中获得目标以及相应内涵，用于不良信息处理
情绪识别（ER）	通过文本分析、心率、脑电波等方式感知人类的情绪状态
AI 建模（DT）	通过软件沟通物理系统与数字世界
生物特征识别（BO）	通过获取和分析人体的生理和行为特征来实现人类唯一身份的智能和自动鉴别
虚拟代理（VA）	具有人类行为和思考特征的智能程序，协助人类识别安全风险因素

来源：亿欧智库整理

未来挑战：网络安全问题产生的根源在于计算机架构本身，难以避免

◆计算机软件和系统漏洞的存在几乎是不可避免的。微软内部统计数据显示，软件工程师每写1000行代码至少会出现一个漏洞。当利用漏洞的方法被黑客掌握就会带来实际的网络安全风险。越流行、越强大的软件可能存在的漏洞越多。与此同时，计算技术的进步也会带来新形式的网络安全威胁。

亿欧智库：网络安全问题产生的根源



来源：专家访谈、亿欧智库整理

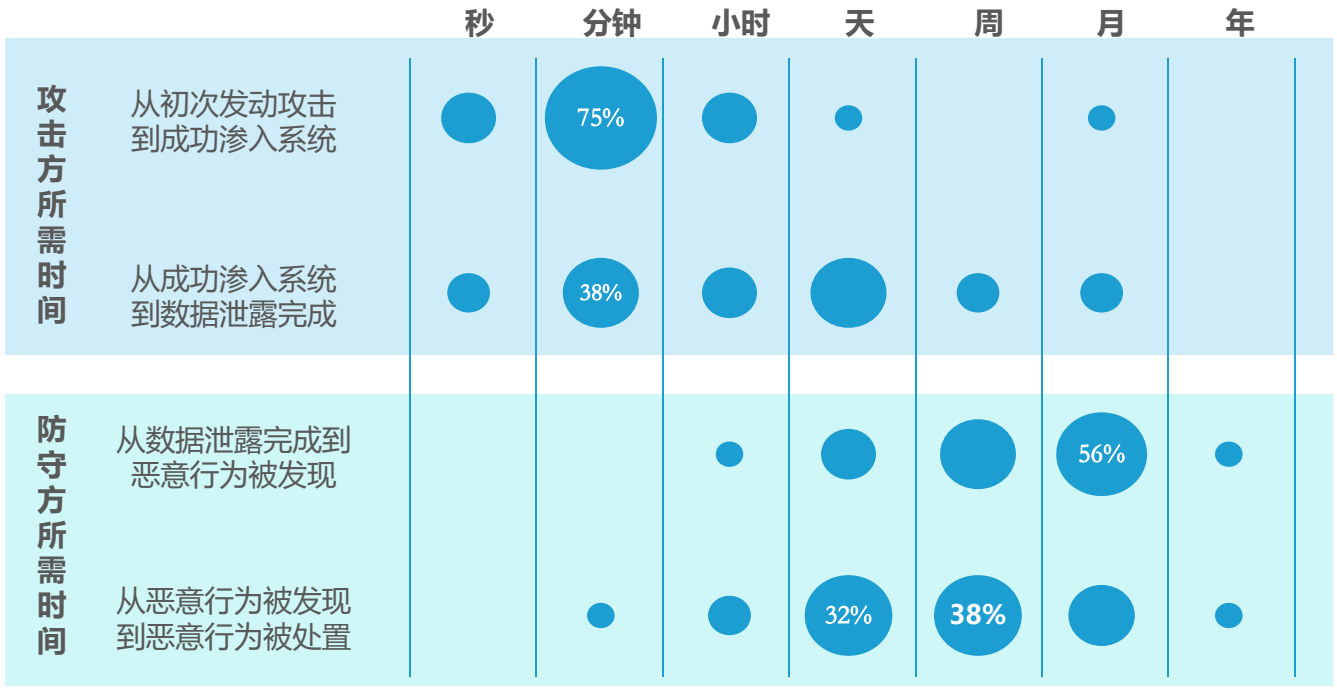
未来挑战：网络安全攻防力量不平衡

◆网络攻防对抗中，信息情报不对称造成的不平衡由来已久。防守方在明处，是一个不能挪动的堡垒，而攻击方躲在暗处，只要有足够的耐心，总是可以找到漏洞和缝隙。尤其随着企业规模不断发展，网络资产体量增加，防护难度加大，攻防之间的不平衡愈发显著。

◆另外，网络安全攻防双方所需时间的数量级存在差异。攻击者从开始攻击到攻陷目标，以及从攻陷目标到窃取数据，往往只需要几分钟；而防护人员从系统被攻陷到发现被攻陷，以及从发现被攻陷到排查恢复系统，往往需要几天、几周甚至几个月的时间。

◆网络威胁态势感知、安全攻防、“杀伤链”模型、白帽测试等策略能一定程度上减轻网络安全攻防不平衡问题。

亿欧智库：网络攻防所需时间数量级比例



亿欧智库：网络攻防“杀伤链”

在真实的网络对抗中，按照“杀伤链”模型，以攻击者——“人”为关注点，从攻击行为、习惯、可能的手段作为出发点进行考虑，往往可以事半功倍。

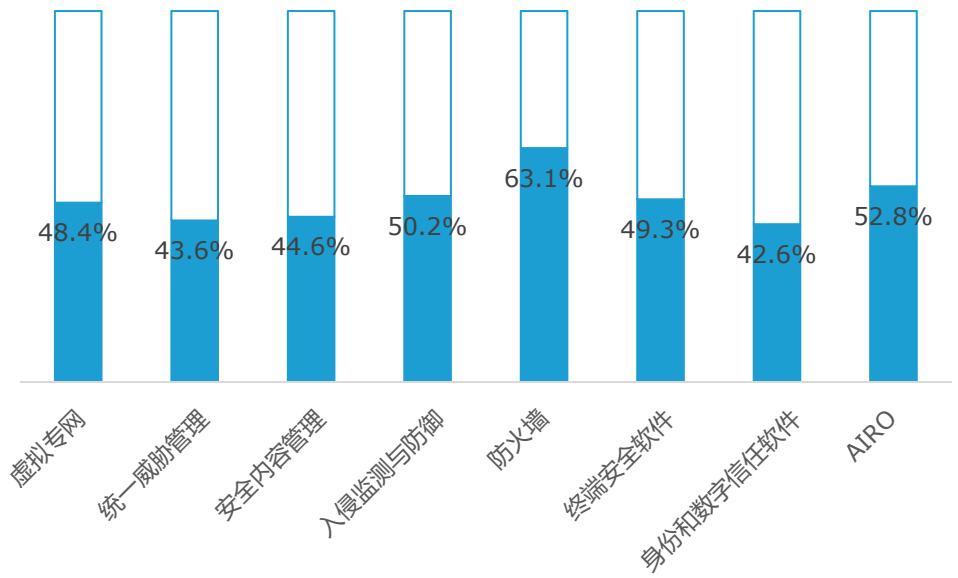
来源：专家访谈、亿欧智库整理

未来挑战：单赛道市场空间有限，全产品线布局难度大

◆网络安全赛道细碎，行业目前呈现缺乏巨头，分散程度高的特点。网络安全企业发展初期多以单点切入，但单一赛道较窄，从总量视角看，单品的市场天花板有限。

◆网络安全企业想要扩大规模，从单点向外扩充产品，再延展目标客户市场是必经之路。在有限市场空间和马太效应的驱使下，安全初创企业可能同时考虑融资和并购两种路径，另外，与大型厂商进行合作，形成产业生态也是初创企业的破局途径之一。

亿欧智库：2018年中国网安行业部分细分赛道前三大企业市占率



亿欧智库：中国网络安全初创企业特点

- •中国初创型安全企业大多围绕云安全、大数据、工业互联网等新安全领域，回避竞争红海，突破传统安全的瓶颈；
- •中国初创型安全企业核心团队多拥有雄厚的技术背景。初创型企业在产品研发上更加聚焦，对甲方用户的定制化安全需求也有更快捷、灵活的响应；
- •虽然早期深耕细分安全领域，初创型安全企业走向壮大也需要依托逐渐完善的产品矩阵，依托需求旺盛的下游行业，塑造有号召力的标杆案例并研发更有针对性的交付产品。

来源：专家访谈、公开资料、亿欧智库整理

团队介绍和版权声明

◆ 团队介绍：

亿欧智库（EqualOcean Intelligence）是亿欧EqualOcean旗下的研究与咨询机构。为全球企业和政府决策者提供行业研究、投资分析和创新咨询服务。亿欧智库对前沿领域保持着敏锐的洞察，具有独创的方法论和模型，服务能力和质量获得客户的广泛认可。

亿欧智库长期深耕科技、消费、大健康、汽车、产业互联网、金融、传媒、房产新居住等领域，旗下近100名分析师均毕业于名校，绝大多数具有丰富的从业经验；亿欧智库是中国极少数能同时生产中英文深度分析和专业报告的机构，分析师的研究成果和洞察经常被全球顶级媒体采访和引用。

以专业为本，借助亿欧网和亿欧国际网站的传播优势，亿欧智库的研究成果在影响力上往往数倍于同行。同时，亿欧EqualOcean内部拥有一个由数万名科技和产业高端专家构成的资源库，使亿欧智库的研究和咨询有强大支撑，更具洞察性和落地性。

◆报告作者：

马诗晴

亿欧智库分析师

Email：mashiqing@iyiou.com

宋世婕

亿欧智库分析师

Email：songshijie@iyiou.com

◆报告审核：

孙毅颂

亿欧智库研究总监

Email：sunyisong@iyiou.com

团队介绍和版权声明

◆ 版权声明：

◆ 关于亿欧：

亿欧EqualOcean是一家专注科技+产业+投资的信息平台和智库；成立于2014年2月，总部位于北京，在上海、深圳、南京、纽约有分公司。亿欧EqualOcean立足中国、影响全球，用户/客户覆盖超过50个国家或地区。

亿欧EqualOcean旗下的产品和服务包括：信息平台亿欧网（iyiou.com）、亿欧国际站（EqualOcean.com），研究和咨询服务亿欧智库（EqualOcean Intelligence），产业和投融资数据产品亿欧数据（EqualOcean Data）；行业垂直子公司亿欧大健康（EqualOcean Healthcare）和亿欧汽车（EqualOcean Auto）等。

亿欧服务

- 基于自身的研究和咨询能力，同时借助亿欧网和亿欧国际网站的传播优势；亿欧EqualOcean为创业公司、大型企业、政府机构、机构投资者等客户类型提供有针对性的服务。

创业公司

亿欧EqualOcean旗下的亿欧网和亿欧国际站是创业创新领域的知名信息平台，是各类VC机构、产业基金、创业者和政府产业部门重点关注的平台。创业公司被亿欧网和亿欧国际站报道后，能获得巨大的品牌曝光，有利于降低融资过程中的解释成本；同时，对于吸引上下游合作伙伴及招募人才有积极作用。对于优质的创业公司，还可以作为案例纳入亿欧智库的相关报告，树立权威的行业地位。

大型企业

凭借对科技+产业+投资的深刻理解，亿欧EqualOcean除了为一些大型企业提供品牌服务外，更多地基于自身的研究能力和第三方视角，为大型企业提供行业研究、用户研究、投资分析和创新咨询等服务。同时，亿欧EqualOcean有实时更新的产业数据库和广泛的链接能力，能为大型企业进行产品落地和布局生态提供支持。

亿欧服务

◆ 政府机构

针对政府类客户，亿欧EqualOcean提供四类服务：一是针对政府重点关注的领域提供产业情报，梳理特定产业在国内外的动态和前沿趋势，为相关政府领导提供智库外脑。二是根据政府的要求，组织相关产业的代表性企业和政府机构沟通交流，探讨合作机会；三是针对政府机构和旗下的产业园区，提供有针对性的产业培训，提升行业认知、提高招商和服务域内企业的水平；四是辅助政府机构做产业规划。

◆ 机构投资者

亿欧EqualOcean除了有强大的分析师团队外，另外有一个超过15000名专家的资源库；能为机构投资者提供专家咨询和标的调研服务，减少投资过程中的信息不对称，做出正确的投资决策。

◆ 欢迎合作需求方联系我们，一起携手进步；电话 010-57293241，邮箱 hezuo@iyiou.com

获取更多报告详情

可扫码关注

亿欧智库

网址：https://www.iyiou.com/research

邮箱：hezuo@iyiou.com

电话：010-57293241

地址：北京市朝阳区霞光里9号中电发展大厦A座10层