

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（下）
及TOP50企业榜单

亿欧智库 www.iyiou.com/research

Copyright reserved to EqualOcean Intelligence, December 2021

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，挖掘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。

数字化网络安全产业图谱

上游

中游

下游

基础硬件



软件系统



基础能力



综合类企业



身份安全



端点安全



应用安全



边界安全



安全运维及服务



云安全



数据安全



物联网安全



工控安全



移动安全



党政军

电信运营商



能源企业



工业企业



金融企业



教育医疗



目录

CONTENTS

1. 数字化网络安全概念

Digital network security concept

2. 数字化网络安全发展形态

Development pattern of digital network security

3. 政府数字化网络安全应用分析

Application analysis of government digital network security

4. 企业数字化网络安全应用分析

Application analysis of enterprise digital network security

5. 机遇与挑战

Opportunities and challenges

政府数字化网络安全应用分析

Application analysis of government digital network security

政府数字化转型现状：数字政府建设初见成效，业务效率大幅提升

◆随着数字政府建设进程快速推进，中央和地方的数字政府建设规划和工作方案陆续出台、建设执行逐步落实。**截至2020年底，中国数字政府的建设已初显成效**，在创新政府治理和服务模式、提升行政管理和服务效率，提高政府公信力和执行力等方面发挥的作用越来越明显。

亿欧智库：2020年政府治理数字化转型进展

顶层设计和方案规划逐渐完善

- 中国有23个省级（**占比71.9%**）和31个重点城市（**占比96.9%**）地方政府明确了政务数据统筹管理机构。
- 16个省级（**占比50.0%**）和10个重点城市（**占比31.3%**）政府已出台并公开数字政府建设相关规划计划、方案意见。

数据开放平台建设稳步推进

- 多地积极推进数据开放平台建设，**56.3%的省级政府、73.3%的副省级政府、32.1%的地级市政府**已依托政府门户网站建立政府数据开放平台。

集约化和协同管理更加深入

- 全国政府网站数量由2015年的84094个集中整合至14475家，基层政府网站的运维能力得到明显提升。
- 全国32个省级政府均建成全省统一的互联网政务服务平台和全省统一的政务服务App，各省互联网政务服务平台均与国家平台实现互联互通。

公共服务数字化转型加快

- 医疗、教育、交通、社保、公共资源交易等公共服务领域的数字化转型成果显著。
- **32个省均建立教育资源公共服务平台**，中国数字教育资源公共服务体系基本建成。

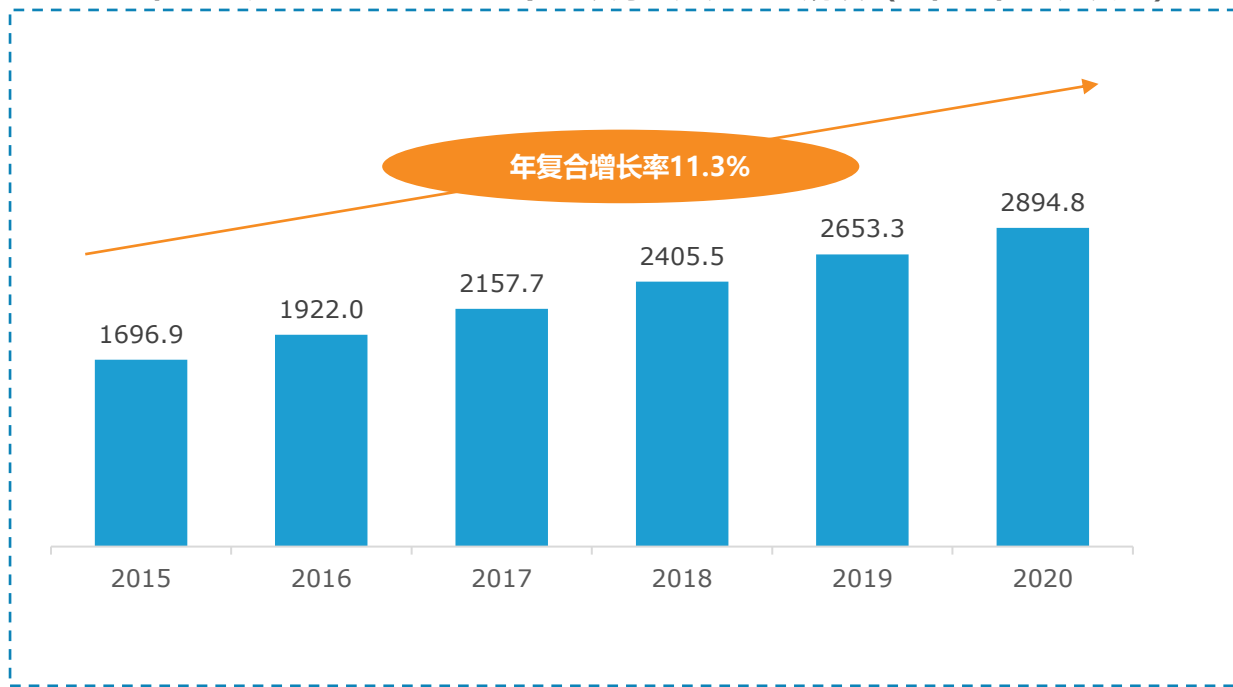
政府网络安全现状：新冠疫情、国际局势影响，政府网站频繁遭受攻击

◆随着数字政府的持续推进，以及各类数字化手段的深入运用，政府治理也正在面临越来越大的网络安全风险。在新冠疫情影响、国际局势复杂的背景下，2019-2020年，**针对中国党政机关和关键信息基础设施等重要单位发动的DDoS攻击组织性和目的性更加明显**，整体呈现高频高发之势。

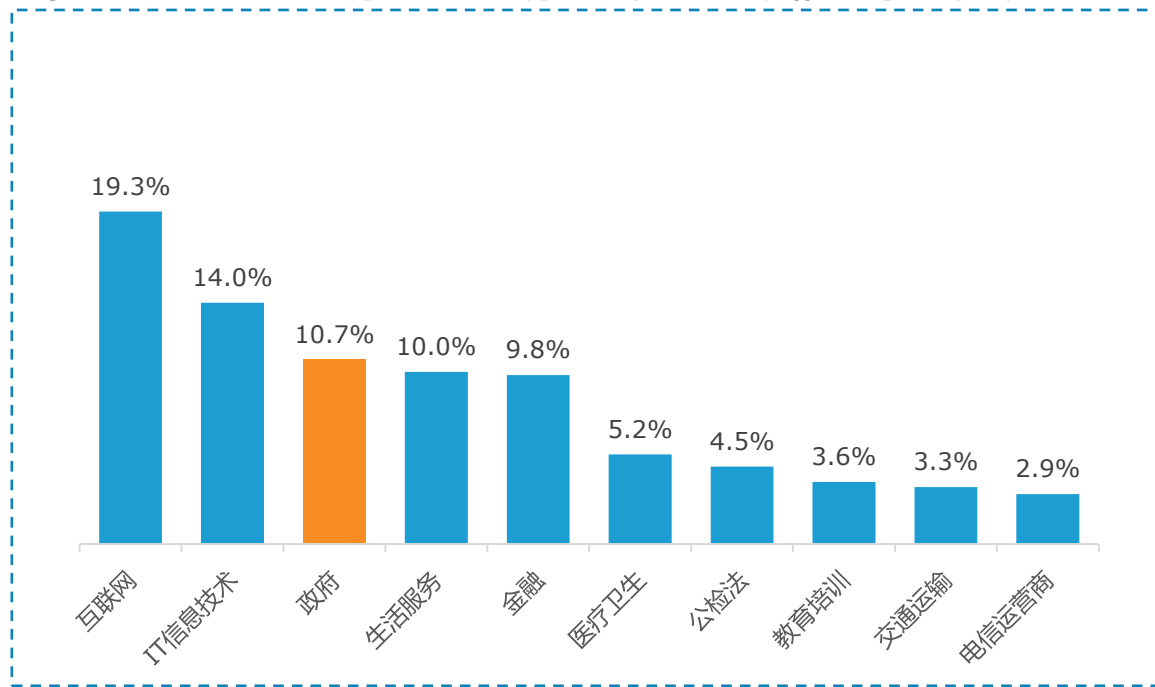
2019年，中国重要党政机关遭受APT组织钓鱼邮件攻击达50多万次，在中国重大活动和敏感时期尤为猖獗。**2019年，中国境内有515个政府网站被篡改。**

◆根据《中国政企机构数据安全风险研究报告》，2019年1月-2020年8月，全球重大数据安全事件中，19.3%发生于互联网行业；14.0%发生于IT信息技术行业；**10.7%发生于政府机构事业单位。**

亿欧智库：2015-2020年中国政府IT应用产业规模（单位：亿元人民币）



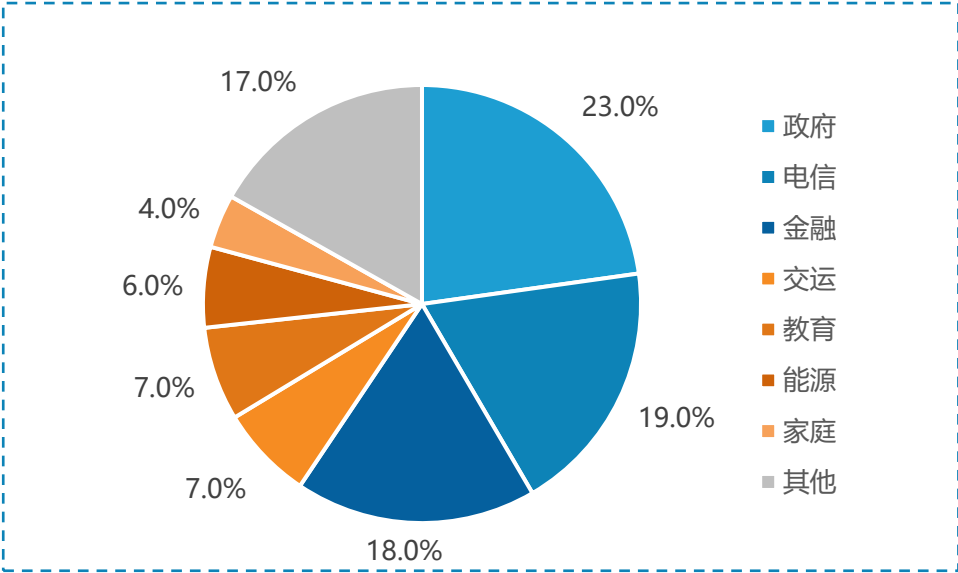
亿欧智库：2019年1月-2020年8月全球政企重大数据安全事件行业分布



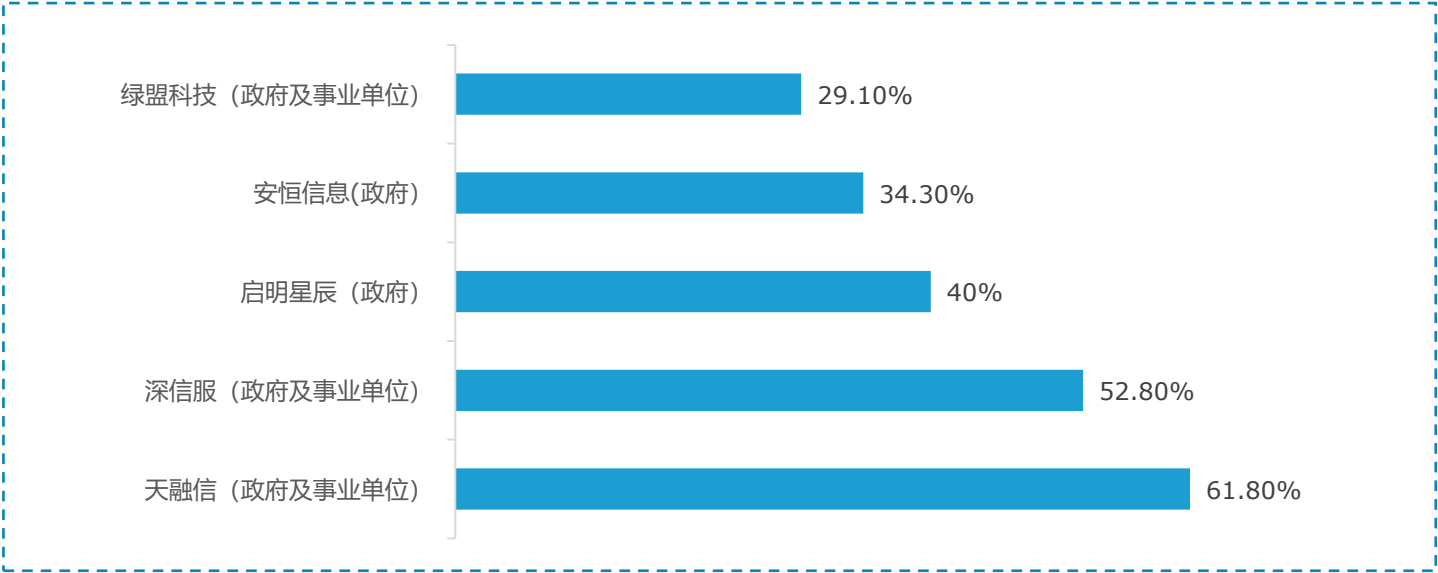
政府网络安全现状：政府成为网安下游市场的最大份额

- ◆数字政府改革建设的重点是推进政务数据的整合、开放和共享，**政务数据和业务的融合集中增加了网络安全防护难度**，使得政府的网络安全建设面临更加复杂的形势和严峻的挑战。
- ◆《信息安全技术网络安全等级保护基本要求》将需要建设等级保护的对象规定为中国境内运营的政府、事业单位、对外提供服务的企业的信息系统，以及基础网络、云平台、大数据、物联网、工控系统和移动互联等领域。
- ◆根据深信服、安恒信息、奇安信、绿盟科技、天融信等大型网络安全厂商披露的数据，**政府通常是他们营收占比最高的下游客户**，2018年平均占比可达30%以上。

亿欧智库： 2018年网络安全下游应用占比



亿欧智库： 2018年主要网络安全厂商政府业务占比



来源：各公司招股说明书、年报，亿欧智库整理

政策制度体系待完善

有关网络安全的政策、法规和各类标准已经逐渐完备，但**各类制度分散在计算机、互联网、信息化建设、计算机软件保护、电子签名、政府信息公开等领域，难以适应当前政府数字化网络安全的发展。**各级机关和各部门单位实际建设落实过程中，仍存在法规、标准不适用、难依照的情况。网安顶层体系设计解决不了基层使用问题，网安建设效果仍需提升。

网络安全基础不平衡

行业主管部门、沿海地区及经济发达地区网络安全能力水平不断增强，而**基层政务部门网络安全意识薄弱，安全基础发展的区域性差异较大。**尤其是基层政务、内陆及经济落后地区网络安全防护水平较弱、责任意识不强，网络安全等级保护等重点工作落实不到位。网络安全防御需要全线配合，在互联互通的大背景下，易引发短板效应，亟需整体提升网安基础，弥补短板。

顶层规划与历史问题难兼容

政府的早期信息系统建设往往各成体系，较为分散，缺乏统一规划。部分单位系统老旧，亟待更新，不再使用的信息系统也未能及时下线仍保存大量重要数据。随着机构改革、业务整合、政府数字化工作的推进，**老旧系统、零散系统的网络安全无法总体统筹规划和设计，成为数字化网络安全薄弱环节。**

政务数据“不敢用、不会用”

政府数字化建设带来的政务数据有着权威性、专业性、全覆盖、可追溯的特征，是非常重要的要素资源。政府数据开放平台累计已达142家，但是数据利用程度较低。**政务数据的安全防护比较薄弱，数据的完整性、保密性和可用性极易遭到破坏。**制度标准、技术手段的不完善一定程度上造成了政府政务数据“不敢用、不会用”的问题。

基层人员安全意识不足

由于政府部门工作人员大部分并不具备系统性的网络信息安全知识，从意识上缺乏整体安全观念。同时受限于客观原因，**很多政府部门工作人员没有机会接受较为系统性的安全意识培训，难以在网络信息安全工作上形成合力**，导致日常工作无人负责，出现问题互相推诿责任，无法有效解决存在的问题及隐患。

经费保障缺乏

网络设备及安全设备的购置、维护、技术支持及软件系统的改扩建都需要经费开销，**使用的经费往往无法直接带来经济效益或社会效益**。政府部门负责人，特别是主要领导难免会对本单位网络信息安全的现状认识不足，形成对安全工作的投入和管理难以满足安全防护要求的局面。

应急能力薄弱

由于各政府部门内部组织架构各不相同，负责网络信息安全的内设机构往往与负责具体业务系统的部门相互平等而又独立，**没有上下管理权力，导致无法形成统一的应急处置流程**，面对突发事件网络信息安全部门和业务部门缺乏信息报送机制，无法及时有效地形成合力处置事件。

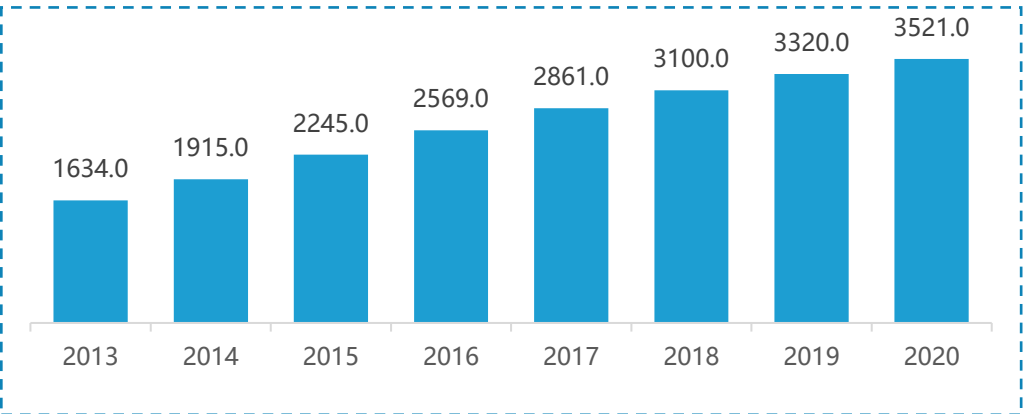
网安人才不足

中国网络安全专业人才缺口预估在50万以上，而每年网络安全相关专业的高校毕业生规模仅2万余人。数据显示，在多个行业受到疫情冲击，招聘规模明显缩减的大背景下，2020年全年，网络安全人才需求量仍较2019年同比增长47.5%。人才需求高速增长，对人才的职业能力要求不断提高，**但人才供给增速始终低于需求增速**，人才质量也难以满足需求。

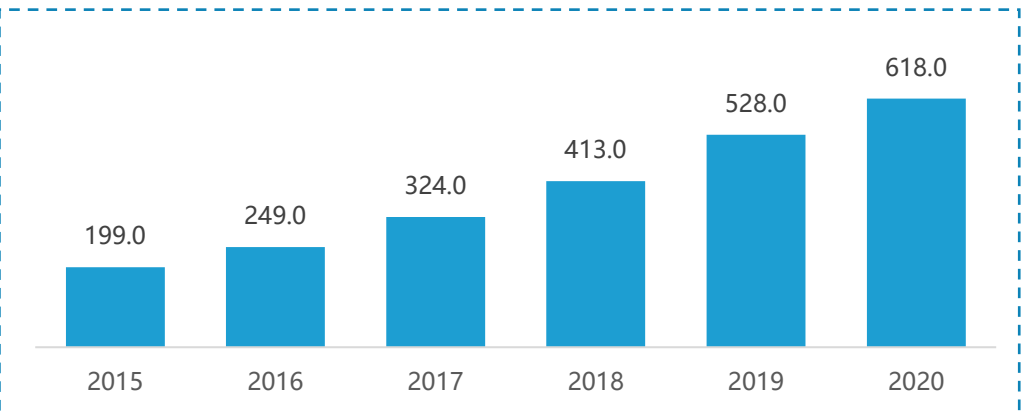
电子政务数字化背景：2020年电子政务市场规模达3521亿元

◆ 电子政务的含义是以信息化手段打破部门间和部门内部的信息孤岛和数据烟囱，重塑、优化政务业务流程和组织体系，打造更加透明、高效的服务型政府，是深化“放管服”改革的重要环节，是推进国家治理体系和治理能力现代化的重要战略支撑。电子政务的重要载体是政府门户网站和政务服务平台，以及背后作为支撑的大数据服务和云服务平台。电子政务的发展目标是打造整体联动、高效惠民的数字政府。

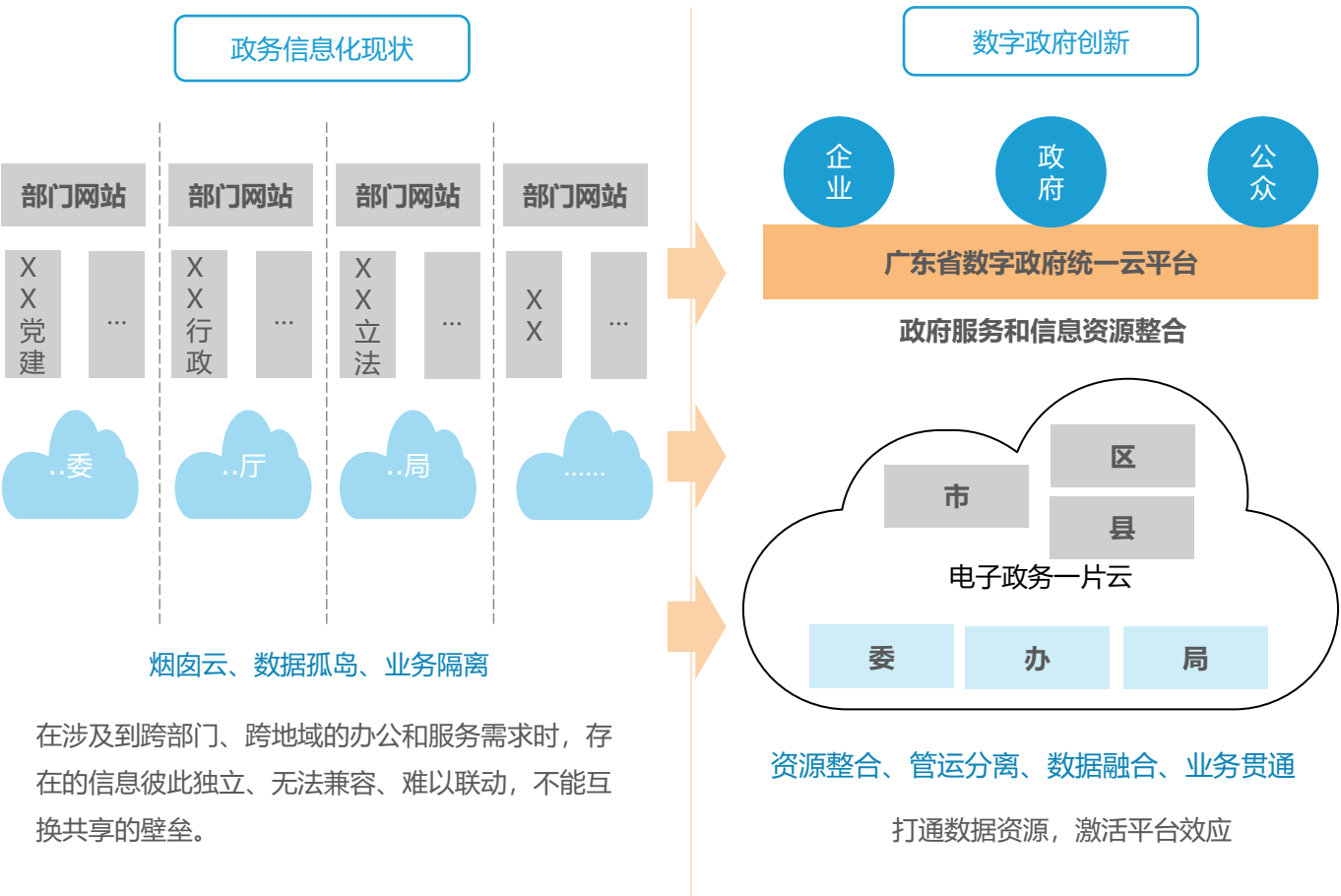
亿欧智库：2013-2020年中国电子政务市场规模（单位：亿元人民币）



亿欧智库：2015-2020年中国政务云市场规模（单位：亿元人民币）



亿欧智库：广东省数字政府建设及运维模式创新



来源：《2018 年广东省“数字政府”改革建设报告》、亿欧智库整理

电子政务网络安全风险：政务上云带来新的风险类别

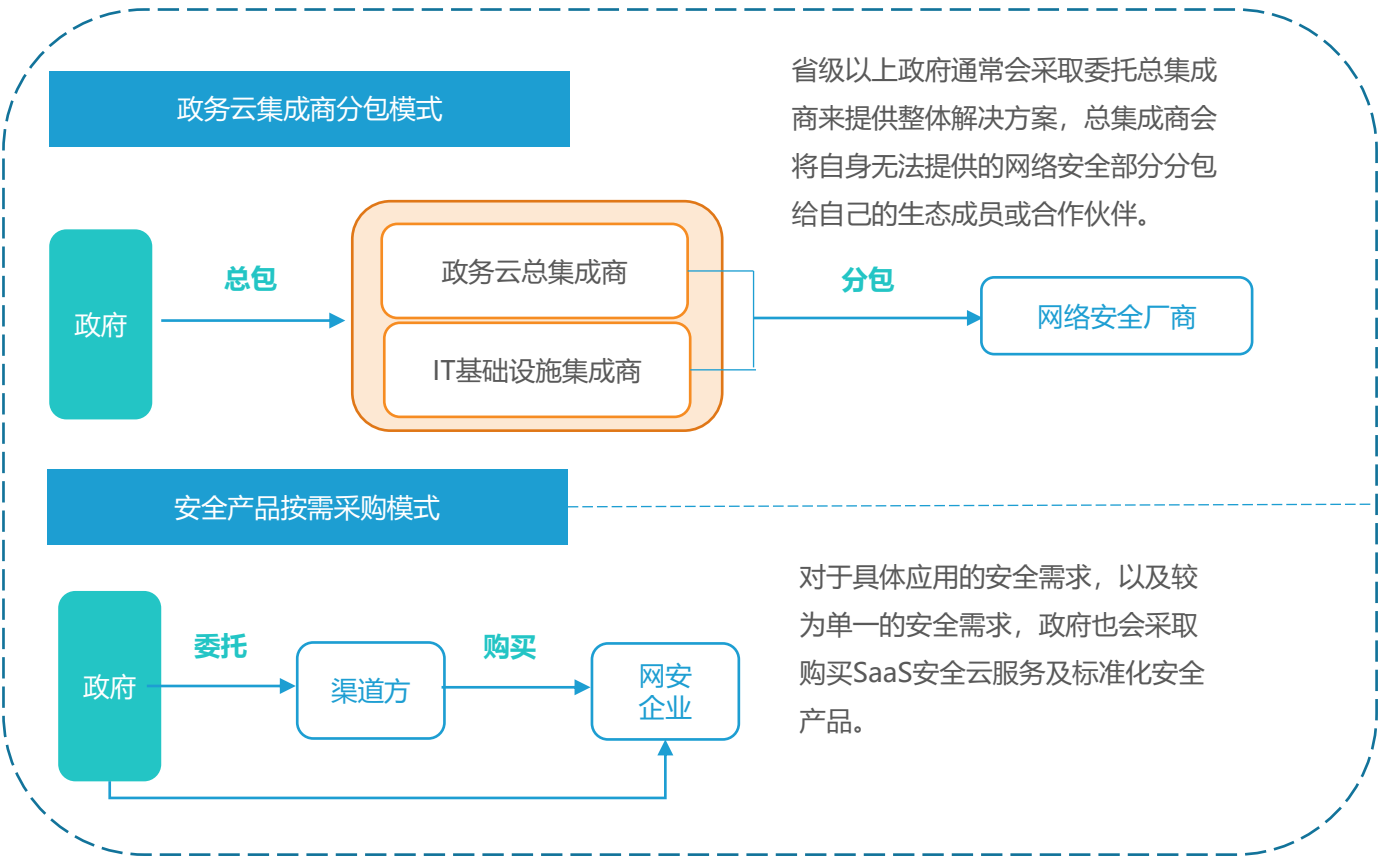
◆国家正鼓励政府部门探索基于云计算的政务信息化建设运行新机制，来推动政务信息资源共享和业务协同。政务云的建设过程中，安全是一个不可忽略也无法绕过的关键问题。保证电子政务系统的安全不仅仅在于可以提供稳定可靠的政务服务，同时更是国家信息安全的一种直接体现。

◆政务云是政务系统和云计算的结合。在政务云环境下，针对云计算和虚拟化技术引入的新威胁与新风险，必须采取一些针对性的防护措施，对核心资产予以保护。

亿欧智库：政务云风险及安全责任划分



亿欧智库：政务云安全解决方案类型

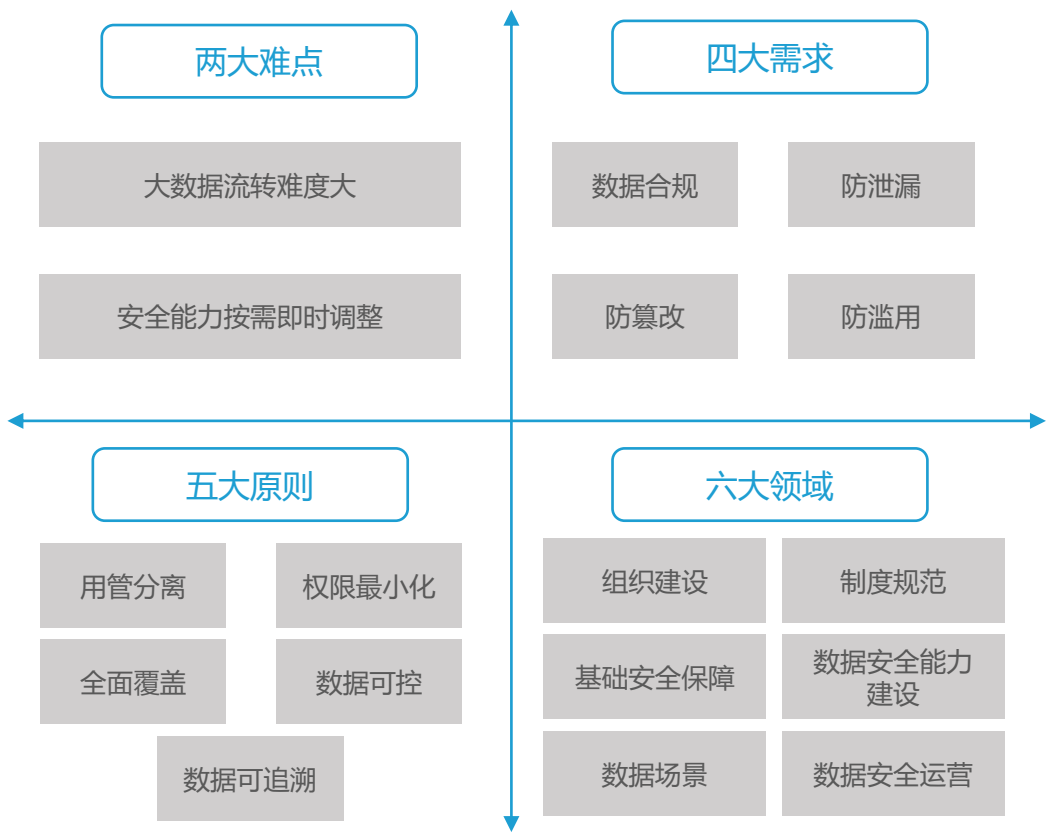


来源：专家访谈、亿欧智库整理

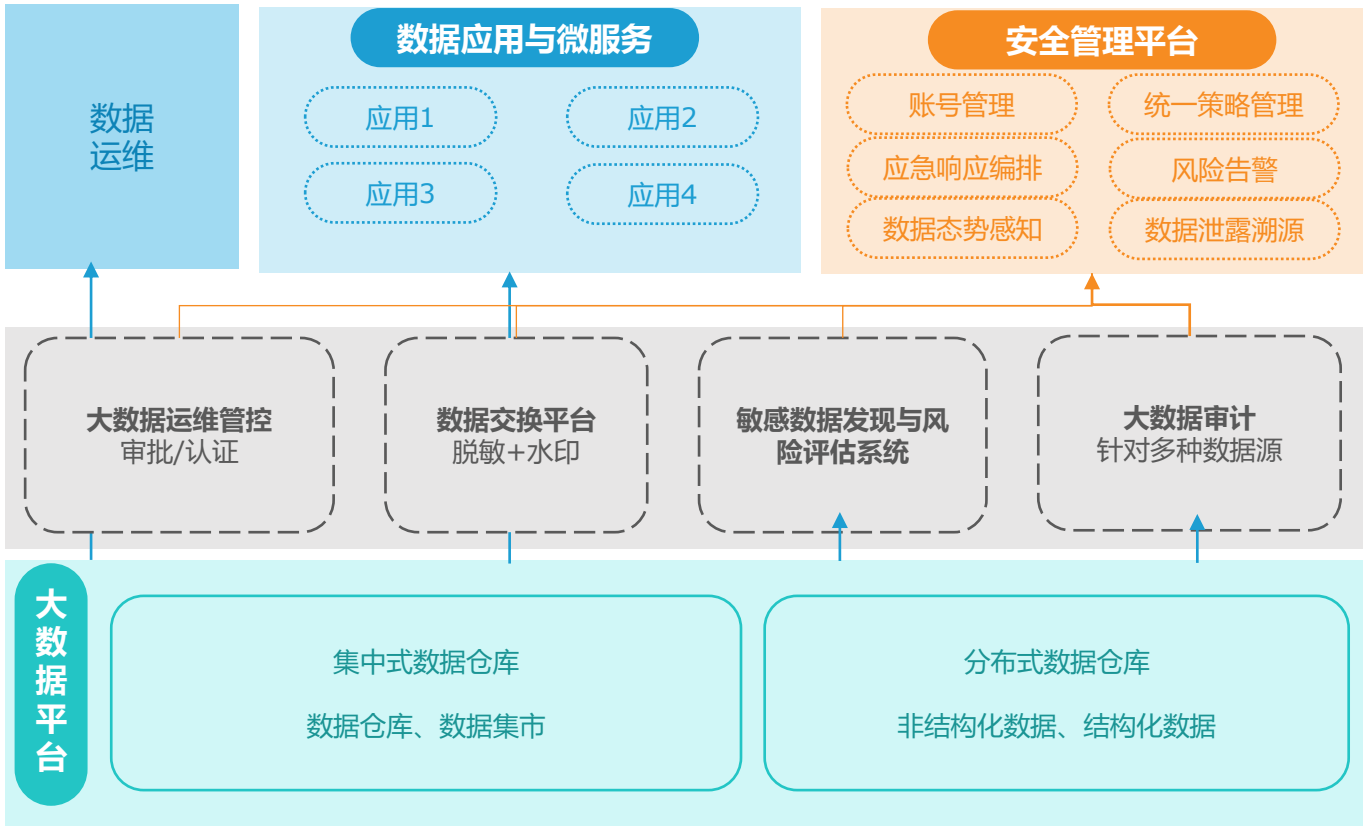
电子政务网络安全建设重点：政务大数据防护难度高、合规压力大

- ◆电子政务和数字政府建设强调要以数据为驱动。据统计，截至2020年底，已经至少有19个省级机构设立了大数据管理机构。
- ◆大数据时代下的政务数据使用具有场景复杂、数据用户多、数据量大、暴露面大等显著特点，面临防护难度大、合规压力大的双重难点。政务数据安全的挑战主要有：
1.数据集中存储且不停地被调用，数据活跃度会增高，流转风险加剧。
2.政务大数据平台的数据体量、格式、活跃度一直在变化，需要据此对安全能力做出相应的调整。

亿欧智库：政务大数据安全要点



亿欧智库：政务大数据安全解决方案

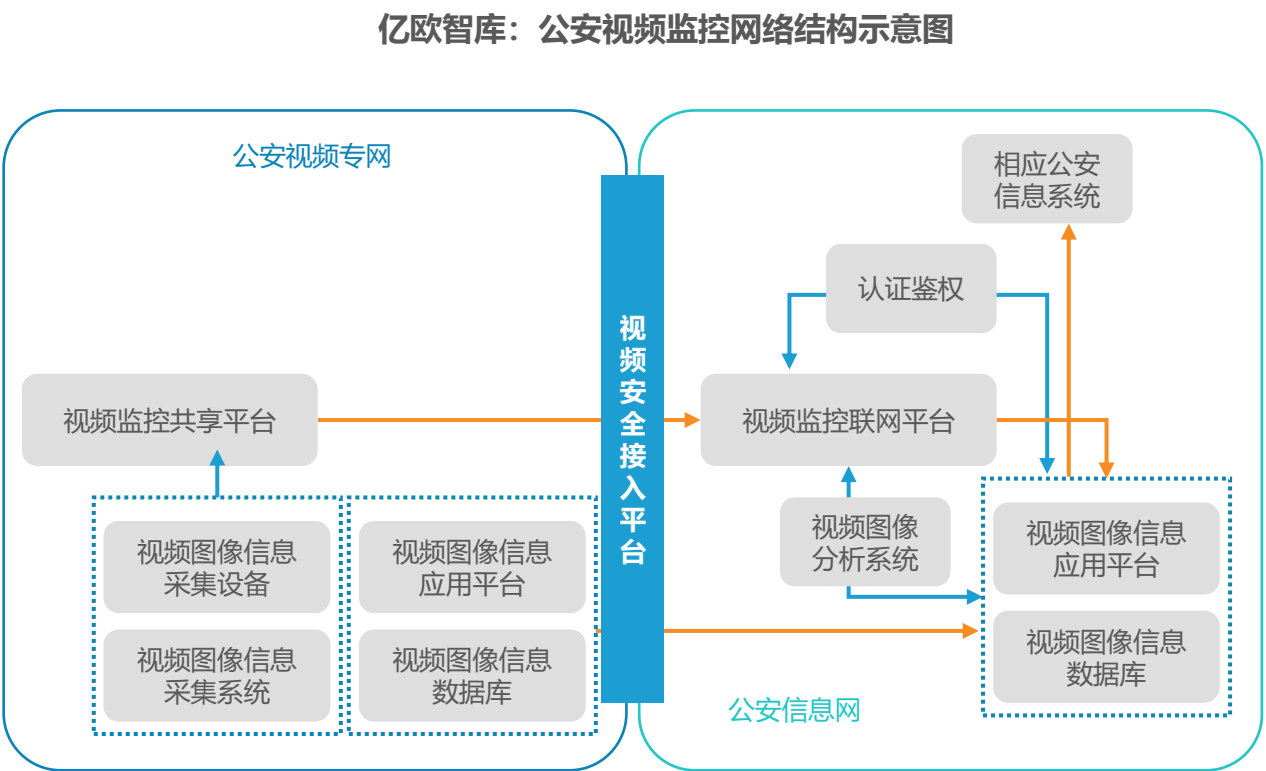
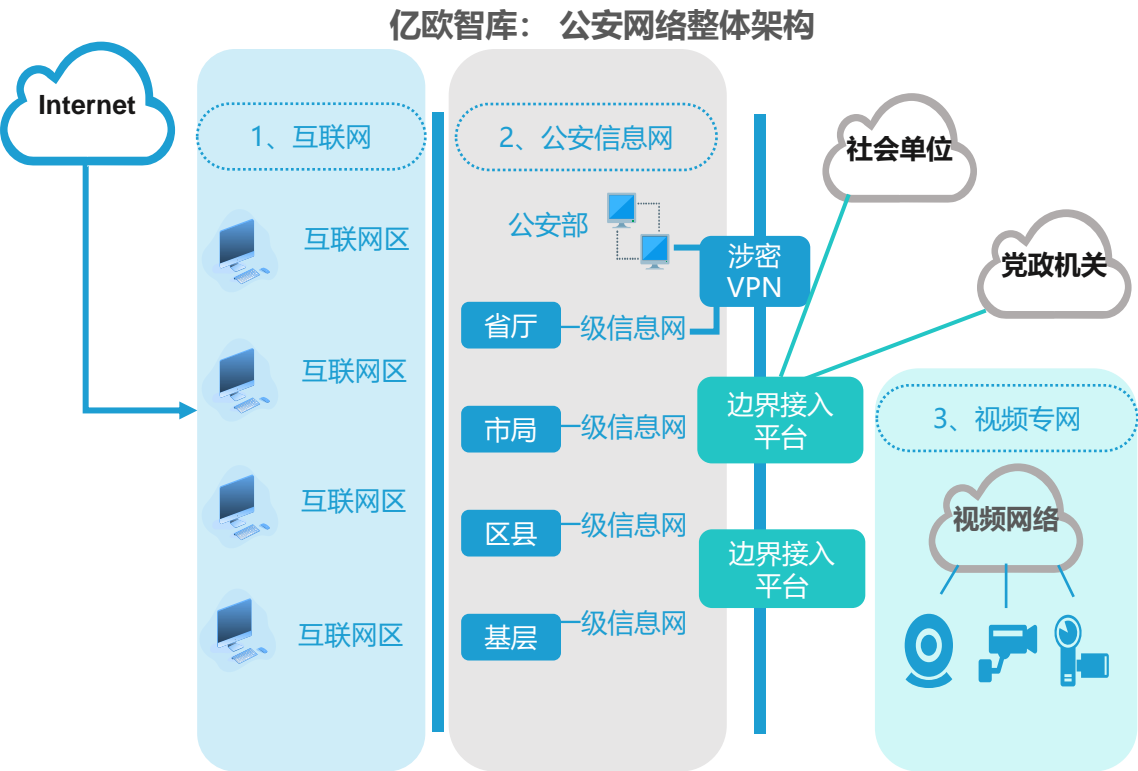


来源：腾讯云、绿盟，亿欧智库整理

公安数字化转型背景：互联网、公安内网和视频专网构成复杂网络结构

◆公安信息系统网络建设主要包括公安基础通信设施和网络平台建设、公安计算机应用系统建设、公安工作信息化标准和规范体系建设、公安网络和信息安全保障系统建设、公安工作信息化运行管理体系建设和全国公共信息网络安全监控中心建设等。**公安信息网络通常有三个组成部分，一是承载公安内部业务的公安信息内网，二是承载外网业务的公安互联网；三是专用承载公安摄像头管理的公安视频专网。**

◆公安机关是网络安全的监管部门，不但占据了网安市场相当的市场份额，同时对产业的整体发展起着关键作用。对网安行业来说最重要的几项监管政策，比如等保和护网行动，也都出自公安部，大部分的网络安全政策落地也是由公安部门来监督执行。



来源：猎鹰安全、专家访谈、亿欧智库整理

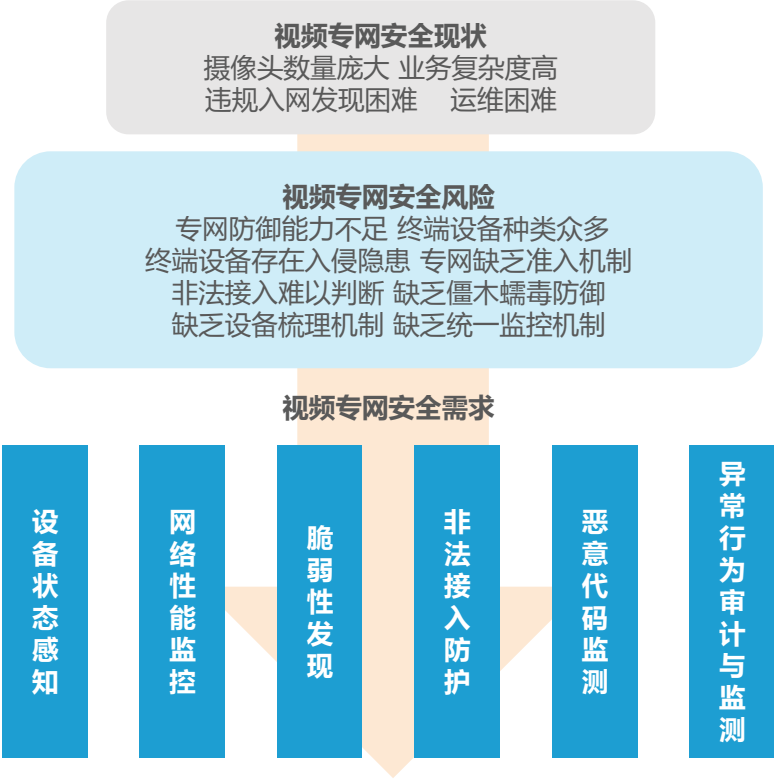
◆雪亮工程，即公共安全视频监控建设联网应用，以“全域覆盖、全网共享、全时可用、全程可控”为总目标，以公安机关视频图像共享平台为核心，分级整合各类视频图像资源，最大限度实现公共区域视频图像资源的联网共享，为反恐维稳、治安防控、应急处理、企业/个体服务、群众服务、城市文明提供强有力的可视化信息支撑。

◆雪亮工程建设不但面临网络安全等级保护监管合规的要求，同时也面临着视频终端设备违规入网，被非法控制，数据中心遭遇恶意入侵攻击，恶意代码传播以及视频数据泄露等安全风险。

亿欧智库：公安网络安全的主要风险点

信息网络结构和边界风险	由于物理隔离不彻底，公安信息可能受到来自互联网访问扫描攻击、DDOS攻击、非法侵入等。
病毒侵害和网络攻击	融合多种攻击手段的病毒和攻击技术成为威胁公安系统的安全风险。
系统安全风险	主要指公安系统采用的操作系统、数据库系统和各种应用系统所存在漏洞的安全风险。
信息传输风险	公安信息传输过程中可能受到非法截取、非法篡改的风险。
公安视频专网风险	针对公安视频专网的非法窃听、系统入侵、越权访问等网络安全风险。

亿欧智库：雪亮工程安全风险及需求分析

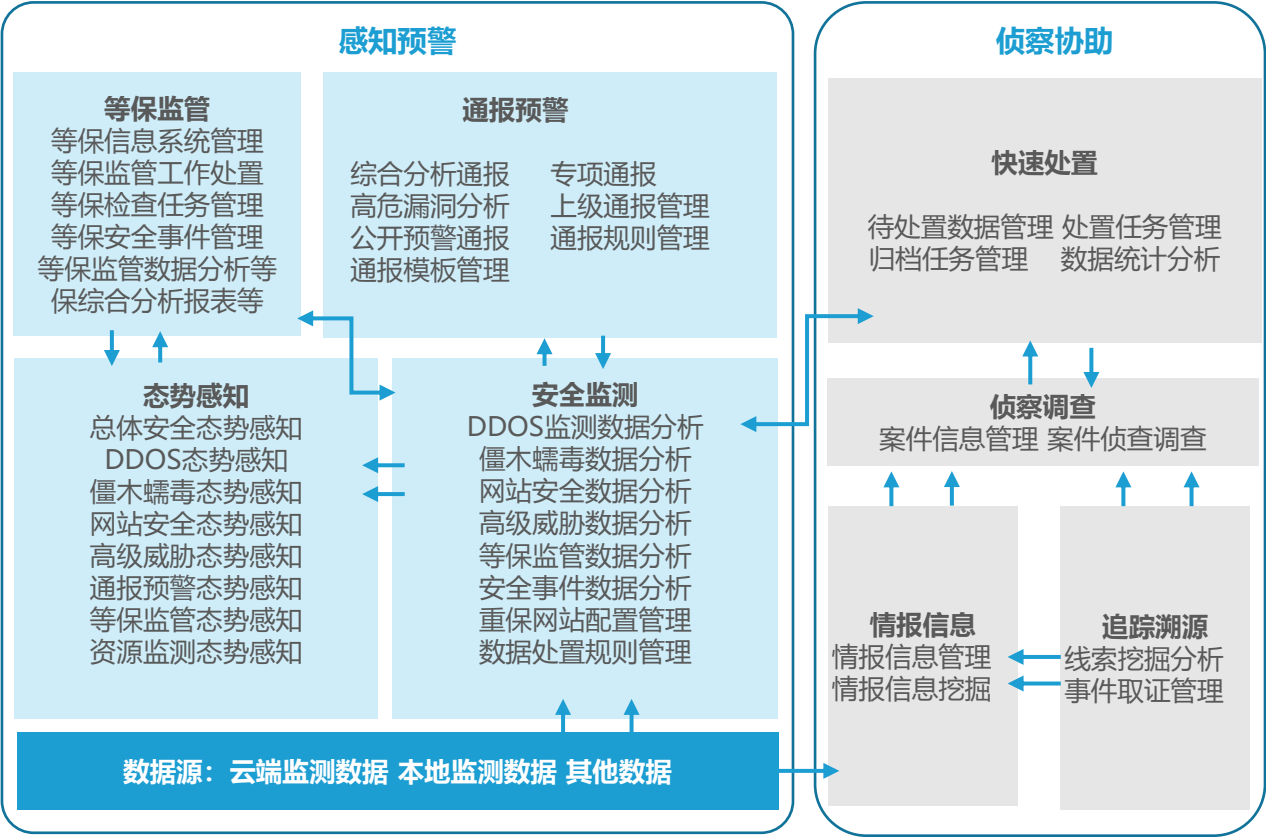


来源： 专家访谈、《公安视频图像信息应用系统（行业标准）》、亿欧智库整理

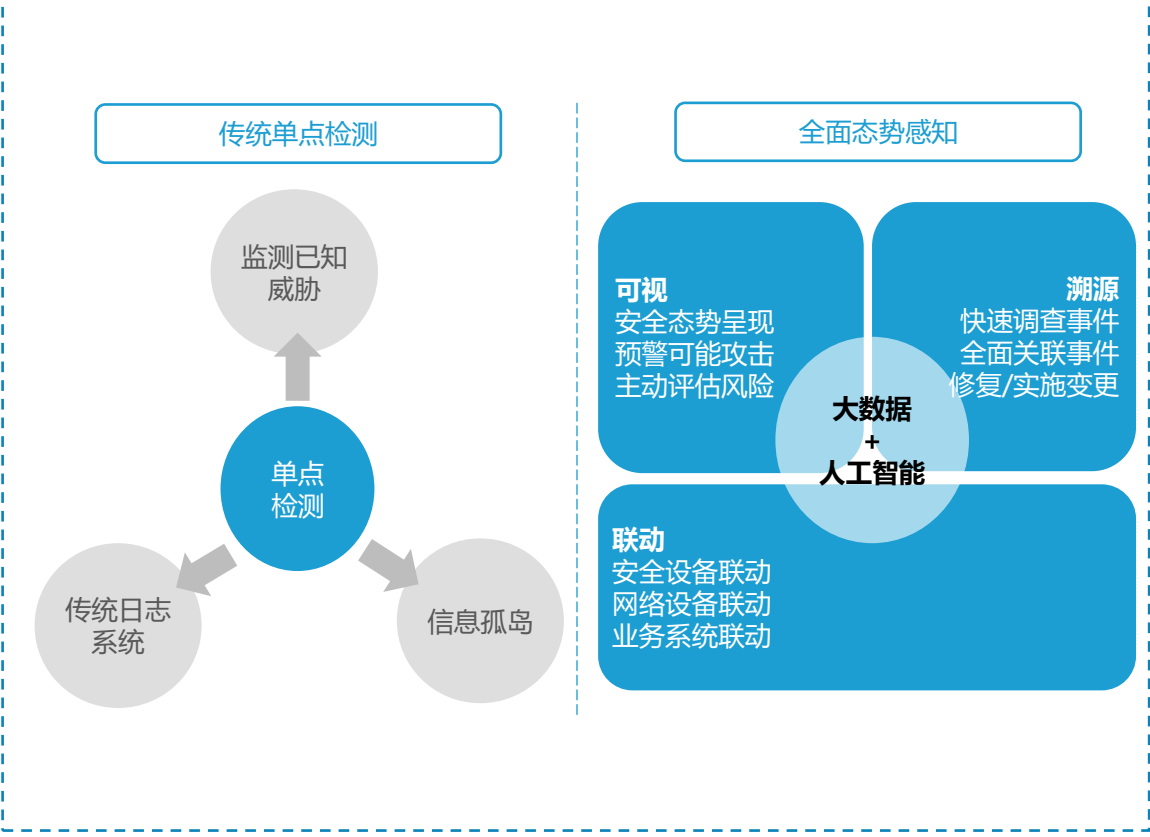
公安数字化网络安全建设重点：监测预警和态势感知技术协助网安监管

◆随着网络技术的发展，各种网络威胁和攻击技术的不断升级，传统的被动式防御网安措施已经不能满足网安防护的需要。**态势感知则是网安主动防御领域的核心技术**，它可以对网络环境中引起网络态势变化的安全要素信息进行获取、理解，评估网络安全的状况，预测其发展趋势，并以可视化的方式展现给用户，帮助用户做出相应的安全决策与行动，从而实现积极主动的动态安全防御。**对于承担网络安全监管职责的公安部门而言，网安监测预警和态势感知成为公安数字化网络安全的重要组成部分。**

亿欧智库：甘肃省公安厅网络安全监测预警和态势感知系统技术架构



亿欧智库：传统单点监测VS全面态势感知

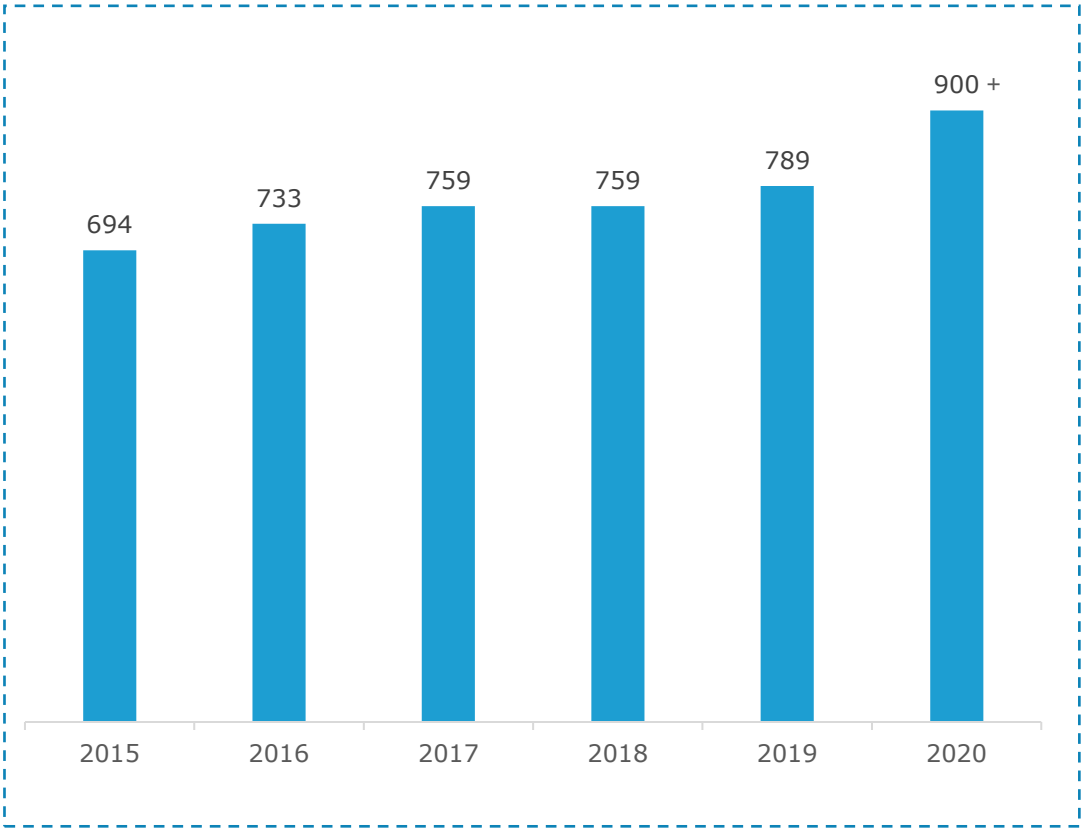


来源： 国家采购招标网，亿欧智库整理

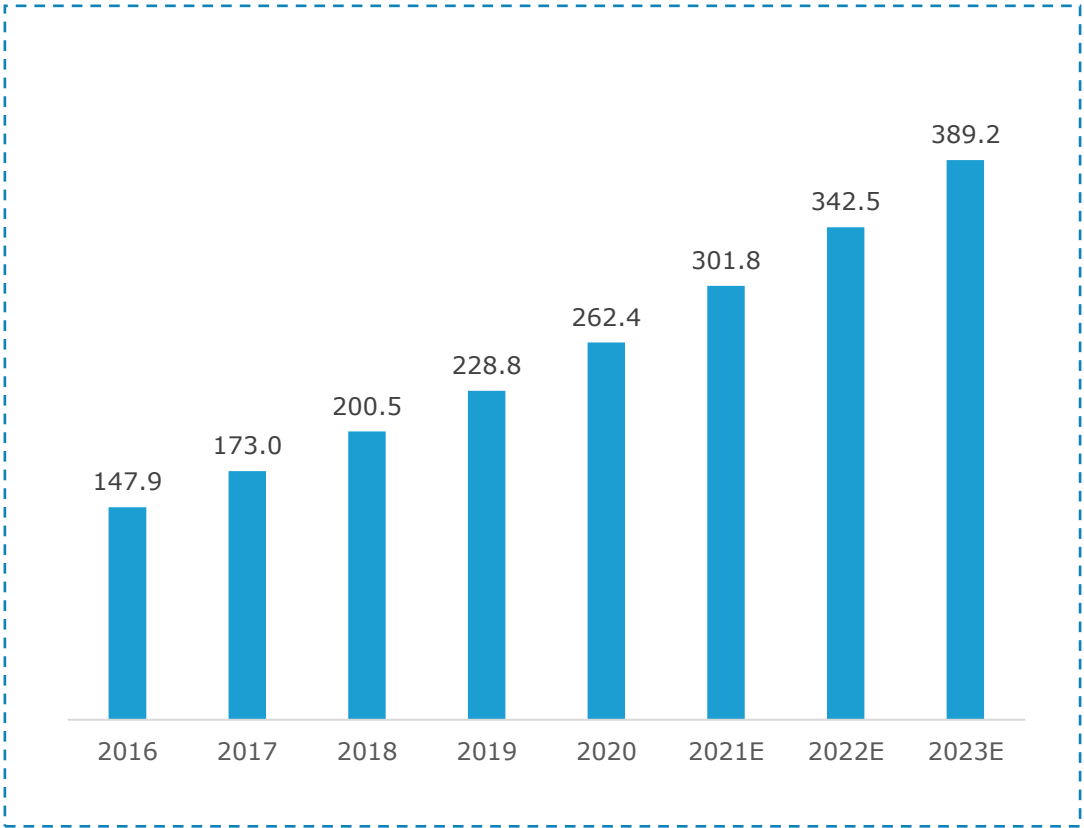
智慧城市数字化背景：建设成果显著，投资规模近300亿元

◆智慧城市是运用新一代信息技术解决城市发展问题，包括管理、民生、经济、政治等多个方面，强调系统、智慧地解决城市化中的问题。中国智慧城市试点已基本覆盖全国各省、市和自治区，其中黄渤海沿岸和长三角城市群较为集中，2020年，中国智慧城市累计试点数量已经超过900个。

亿欧智库：2015-2020年中国智慧城市累计试点数量
(单位：个)



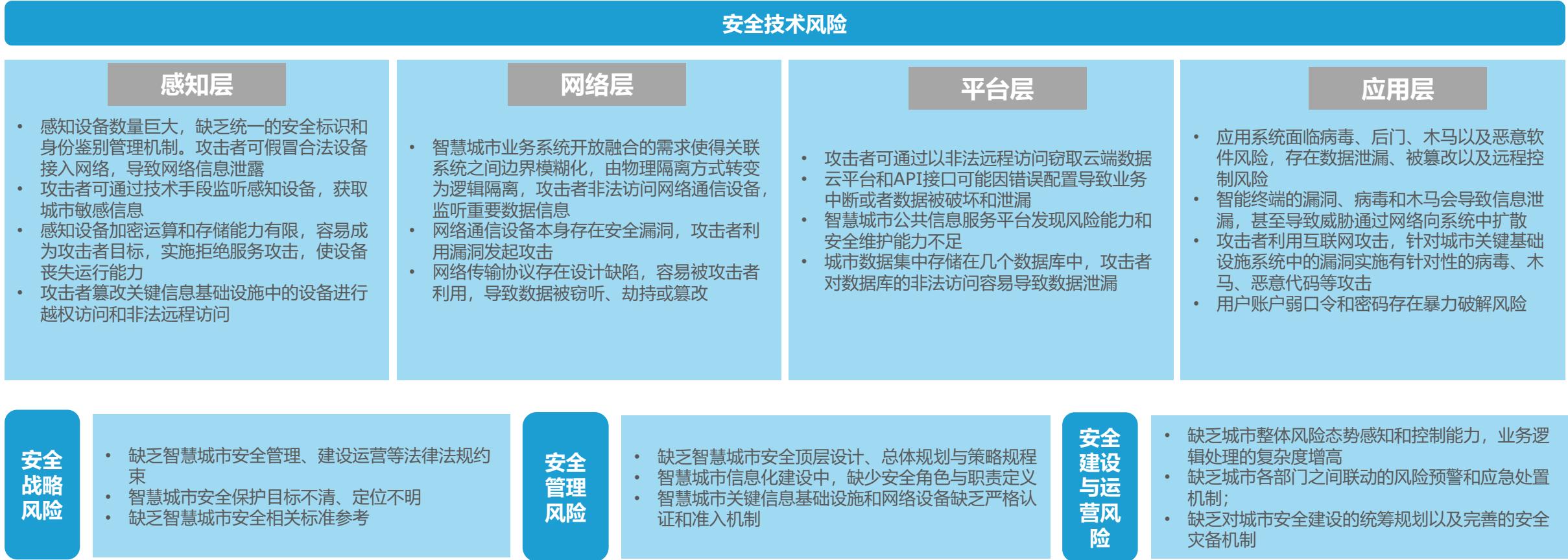
亿欧智库：2016-2023年中国智慧城市投资规模统计
(单位：亿元人民币)



来源：住建部、发改委、工信部、亿欧智库整理

◆按照《GB/T 37971-2019信息安全技术 智慧城市安全体系框架》，智慧城市安全指的是智慧城市中对信息保密性、完整性和可用性的保持，以及依此提供的应用与服务安全。智慧城市面临的安全风险主要体现在以下几个方面：安全战略风险、安全管理风险、安全技术风险和安全建设与运营风险。

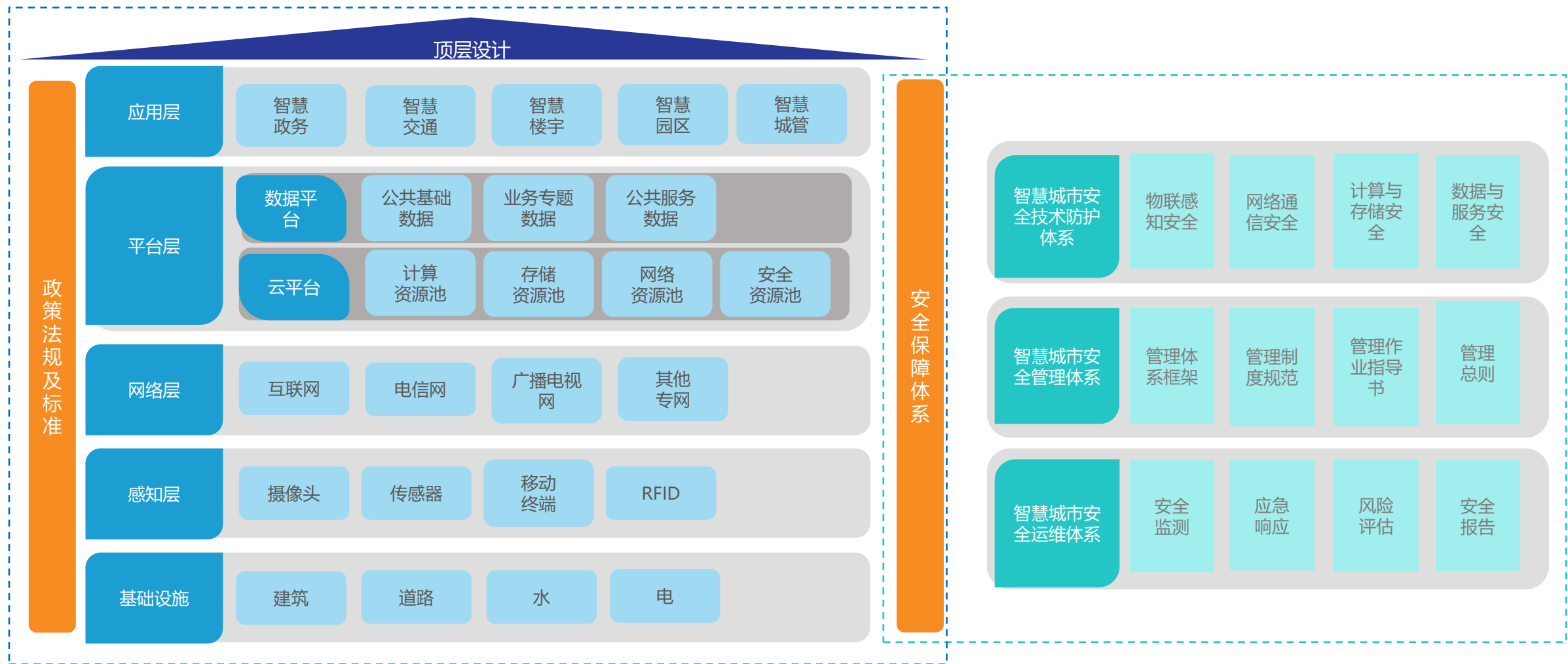
亿欧智库：智慧城市安全风险



智慧城市网络安全建设重点：注重顶层设计，涉及防护、管理、运维

◆智慧城市安全保障体系基于智慧城市顶层设计，覆盖智慧城市建设中的基础设施、感知层、网络层、平台层、应用层，构建智慧城市安全技术防护体系、智慧城市安全管理体系以及智慧城市安全运维体系。

亿欧智库：智慧城市安全防护体系



企业数字化网络安全应用分析

Application analysis of enterprise digital network security

企业数字化转型现状：数字化程度与基础设施建设规模匹配

◆随着中国数字化转型由单点应用向连续协同演进，传统产业利用数字技术进行全方位、多角度、全链条的改造提升。企业数字化转型也呈现出了投入持续加大、技术与业务结合更紧密等特征。根据《2021中国企业数字安全建设白皮书》，中国很多行业都处于“深度数字化依赖”状态，其**数字化建设程度与基础设施建设规模运行相匹配**，而非与员工人数相匹配。

亿欧智库：企业数字化转型现状



企业投入持续加大

数字化转型在企业的战略高度均有提升，众多企业在数字化转型的资金、人才等资源方面投入不断加大。2020年中国数字化转型市场支出大幅提升，同比增长13.6%



业务与技术结合更为紧密

在企业推进数字化转型过程中，业务部门和技术部门结合更为紧密。现阶段企业更多基于自身行业特点和业务发展阶段，寻找到适合企业自身成熟度以及发展战略的数字化转型方案，有针对性地分阶段、分步骤推进。

新兴技术不断涌现并落地应用



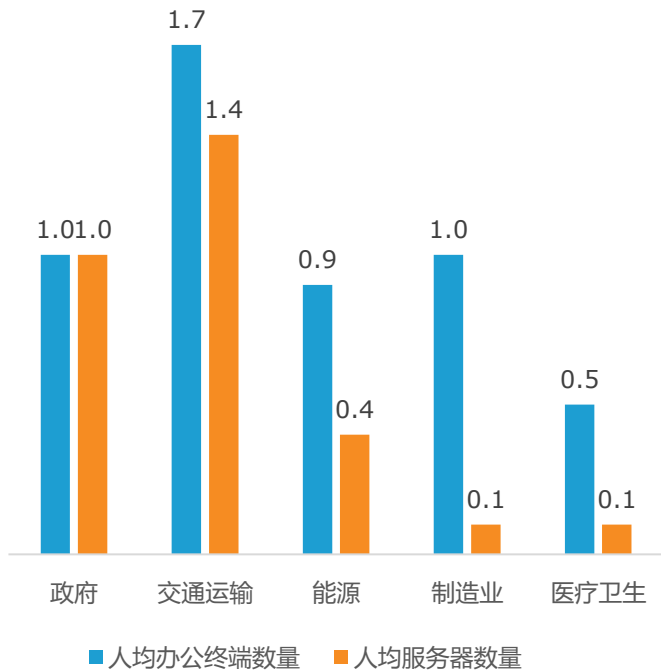
各类新兴技术支撑企业数字化转型，比如5G、AI、AIoT、RPA、区块链、VR、AR等。企业结合自身数字化转型目标，为新兴技术找到新的应用场景，推动财务、生产制造、供应链管理等环节数字化。

疫情推动数字化转型进程



2020年突发疫情加速了各行各业数字化转型进程，在生产方面，工业企业特别是行业龙头持续发力智能制造和工业互联网；在消费方面，全社会消费服务模式加速向互联网迁移，智能家居、在线新零售、智能出行等服务市场迎来新增长。

亿欧智库：2020年各行业企业平均数字化规模
(单位：个)

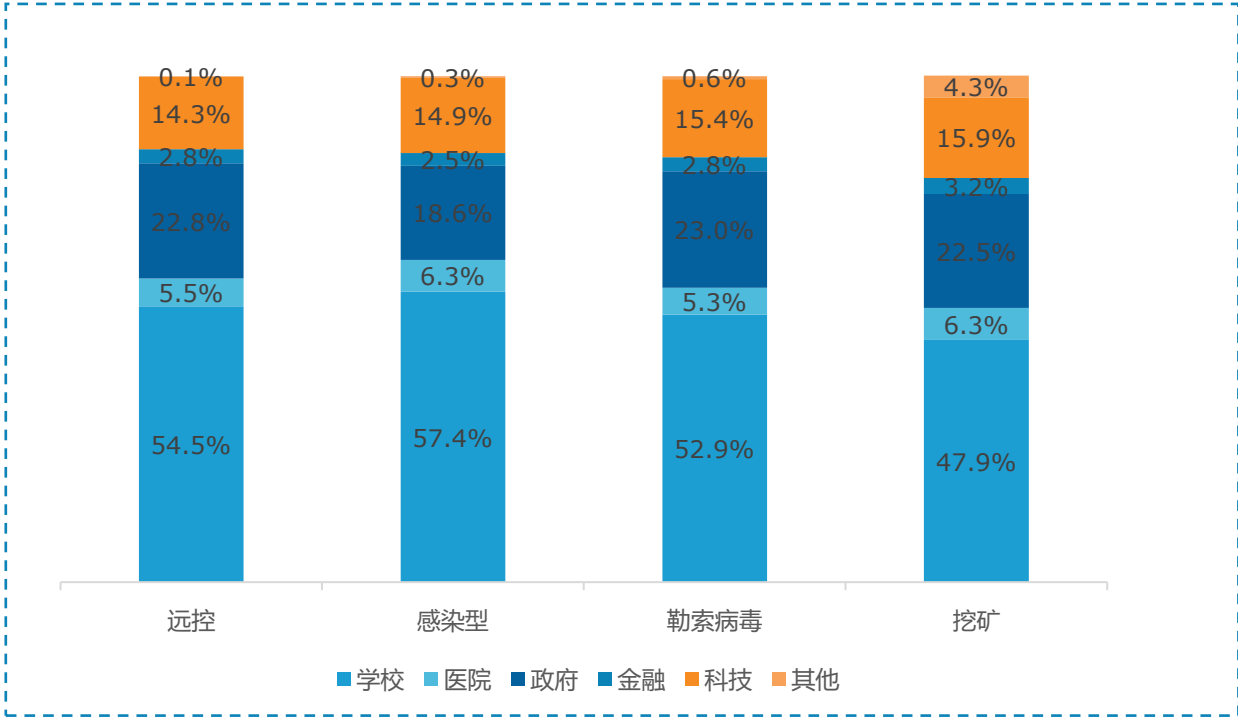


企业网络安全现状：各行业网络风险增加，管理者重视程度逐年提升

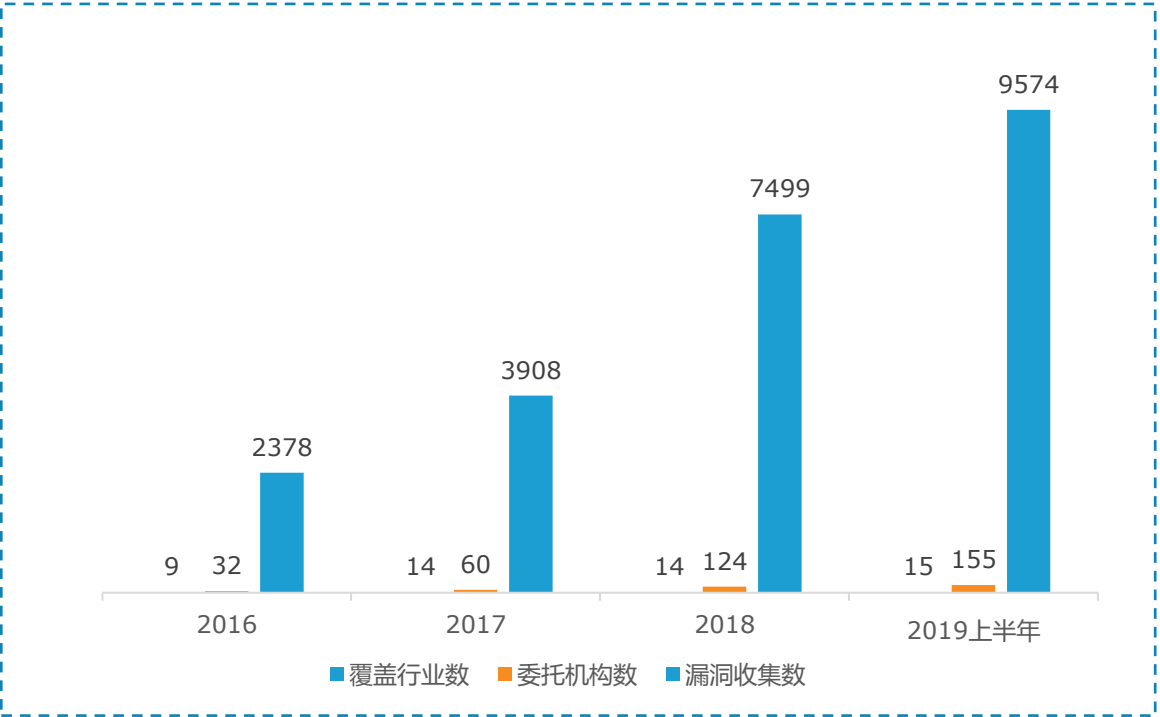
◆随着企业数字化转型不断推进，企业遭遇的网络风险进一步加剧。尤其随着终端增多，被病毒感染的风险进一步增加。**风险木马软件、后门类、感染病毒是企业面临的三大主要威胁**。从行业看，病毒攻击对教育、科技、医疗、金融、政府等行业均有不同程度影响。其中，教育受病毒影响最大，主要由于教育行业存在频繁的文件传输。

◆根据《大中型政企机构网络安全建设发展趋势研究报告》，委托机构数量以及漏洞收集数量都呈现出逐年快速增长的态势，且2019年上半年委托服务的机构数量和漏洞收集数量，超过2018年整年。由此可见，政企管理者对网络安全工作重视程度逐年提高。

亿欧智库：2019年不同类型病毒行业分布情况



亿欧智库：2016-2019上半年大中型政企机构商业委托漏洞挖掘项目数量 (单位：个)



来源： 腾讯安全、《大中型政企机构网络安全建设发展趋势研究报告》、亿欧智库整理

企业安全管理制度不完善

企业安全意识淡薄以及管理制度不完善，导致企业往往在遭遇网络攻击后，再被动部署网络安全产品，起到“打补丁”的作用。但随着企业数字化转型深入，企业对新技术的追求延伸出了新的信息安全风险点，不完善的管理制度一方面将导致安全能力与系统应用能力不匹配，另一方面将面临来自内部人员失误或蓄意破坏、信息窃取风险。

企业对自身资产不清晰

传统的信息安全视角下，信息资产仅硬件、人员、场地服务等方面，但新一代信息技术的发展，使得企业的数据资产数量激增，而企业对于自身存在哪些资产并不清晰，更不用说潜在的网络安全风险。企业网络安全体系要做到事前预防、事中处理、事后追溯，真正落地取得防护效果，需要网络安全服务商对其进行系统化地梳理和设计顶层架构。

企业安全产品呈孤立状态

由于过往企业以“打补丁”的方式部署网络安全产品，导致各网络安全产品或系统之间呈孤立状态，产品效能未能发挥至最大。随着企业数字化转型的深入，企业业务成长，规模扩大，企业网络安全规划需要补齐短板，与企业成长相适配，企业需要具备可持续的安全运营能力。

企业安全人才匮乏

网络安全是一门需要极强综合能力的计算机学科，并且需要非常丰富的实践经验，人才成长周期漫长。随着数字化的推进，企业对网络安全人才需求逐步增长，2019年上半年网络安全人才需求规模较2018年下半年环比增长104.9%，并且存在供求地域失衡的特点，网络安全人才多集中于北上深等一线城市。

制造业数字化转型背景：政策规划全面促进，工业互联网规模快速提升

◆在当今国际形势复杂多变、逆全球化思潮蔓延的局势下，加速实现制造业数字化转型，有助于解放生产效率，促进高端制造业国产替代。近几年，国家出台了一系列政策推动制造业数字化、智能化升级。

◆工业互联网是实现制造业数字化转型的关联路径。根据工信部印发的《工业互联网创新发展行动指南（2021-2023）》，**预计到2025年，工业互联网核心产业市场规模将达到12400亿元，较2020年市场规模增长1倍。**根据工信部《“十四五”智能制造发展规划》，**到2025年，规模以上制造业企业基本普及数字化，重点行业骨干企业初步实现智能转型。**

亿欧智库：《“十四五”智能制造发展规划》主要内容

目标

2025年，**智能制造成熟度**：50%以上企业≥2级；重点行业20%≥3级；重点区域15%≥3级

2025年，**智能制造装备和工业软件技术国产化率**分别高于70%、50%。营收超50亿的系统解决方案供应商>10家

2025年，智能制造行业标准>200个，工业互联网平台>120个

任务

系统创新：
加快攻关核心技术、突破集成技术、建设创新网络

推广应用：
建设智能制造示范工厂、加快行业数字化转型

自主供给：
发展智能制造装备、工业软件、系统解决方案

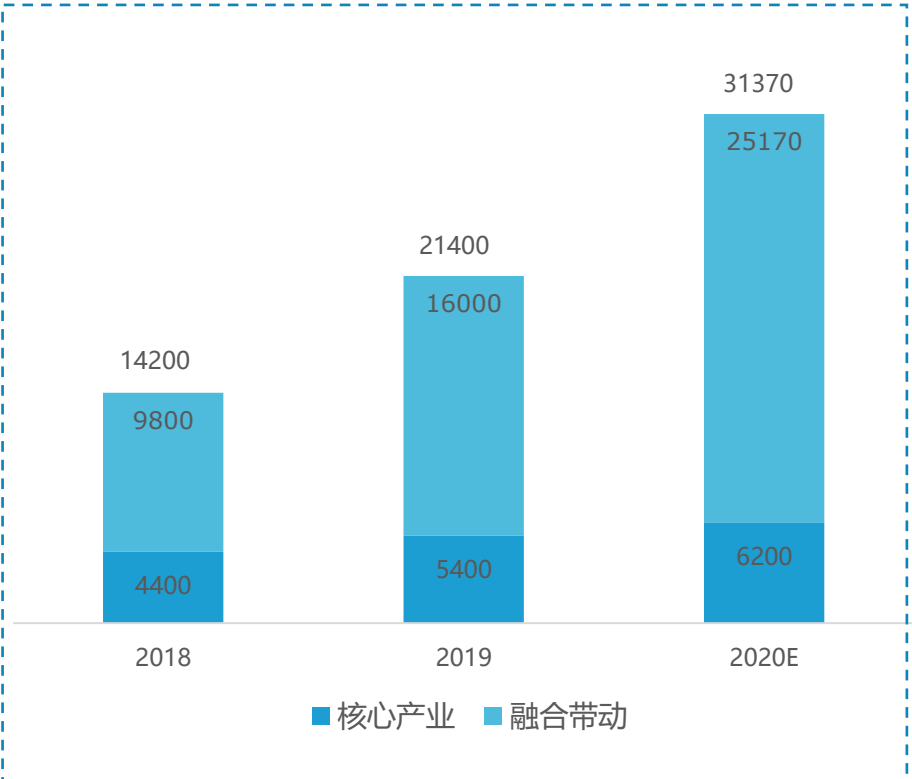
基础支撑：
推进标准化、信息基建、安全保障

行动

新技术应用智能场景>2000个；
标杆智能工厂>100个；
先进智能制造装备>1000个；
遴选标准应用试点单位>100个；

智能车间>1000个；
智慧供应链>100个；
突破开发一批研发设计软件/行业专用软件；
修订国家、行业标准>200个

亿欧智库：2018-2020年工业互联网产业规模
(单位：亿元人民币)



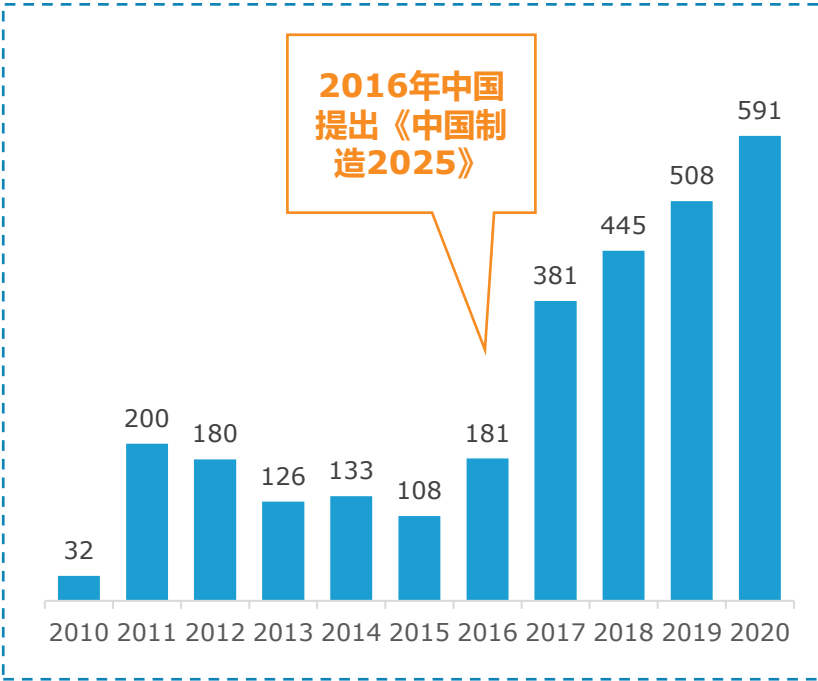
来源：2020年工业互联网大会、亿欧智库整理

制造业网络安全风险：设备高危漏洞隐患大，工业互联网安全形势严峻

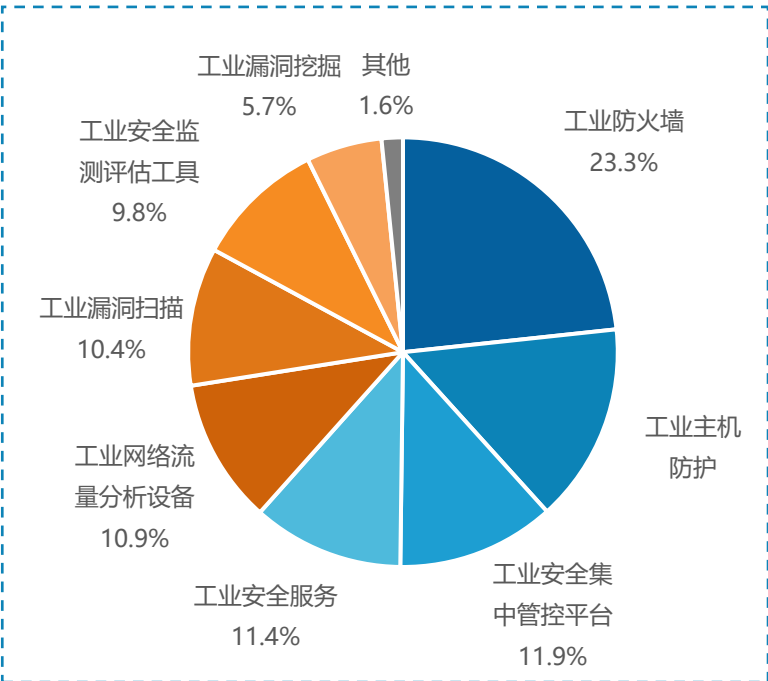
◆根据国家信息安全漏洞共享平台统计，工控漏洞数量伴随新技术应用快速增长。尤其在2016年，我国正式提出《中国制造2025》之后，历年工控漏洞新增数量上了一个新台阶，2020年新增工控漏洞达591个。

◆工业互联网网络安全痛点主要来自于：**一是现实工业系统与互联网技术结合使网络安全和物理安全边界模糊，网络安全风险增大；二是工控系统攻防形式严峻；三是随着合规要求和显示需求增加，企业的网安需求激增，但相应配套资源尚难以匹配。**

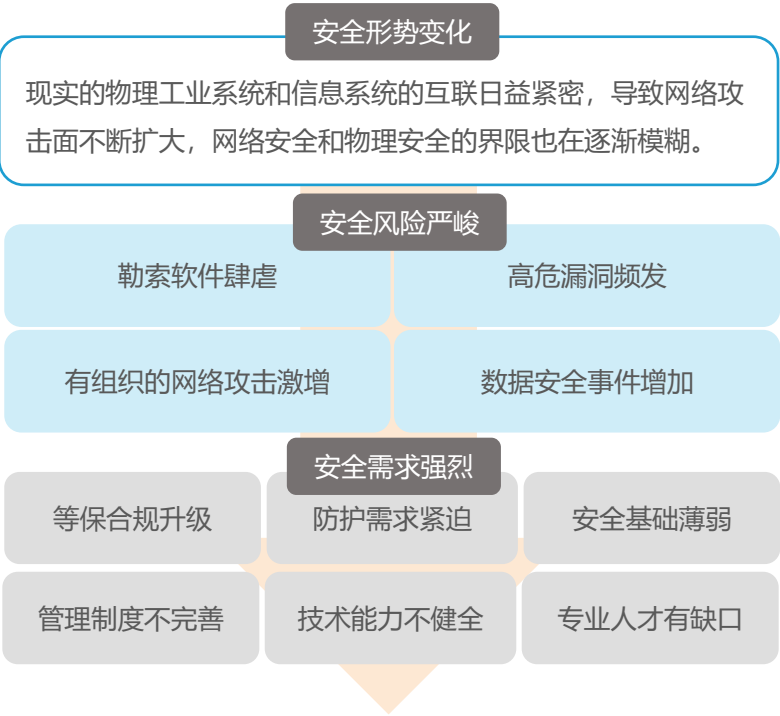
亿欧智库：2010-2020年中国新增工控安全漏洞数量
(单位：个)



亿欧智库：2018年工业互联网安全产品需求占比



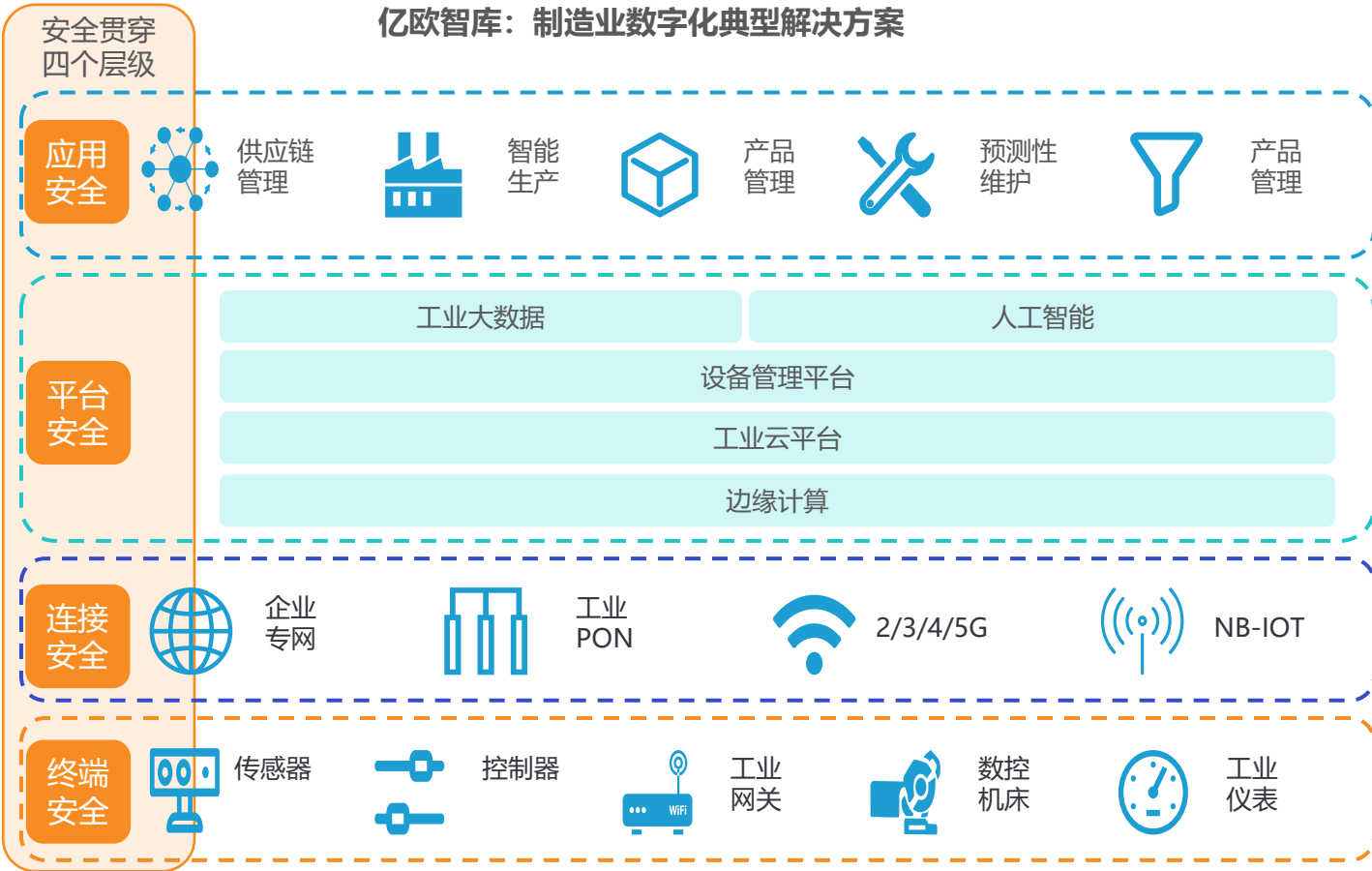
亿欧智库：工业互联网安全痛点



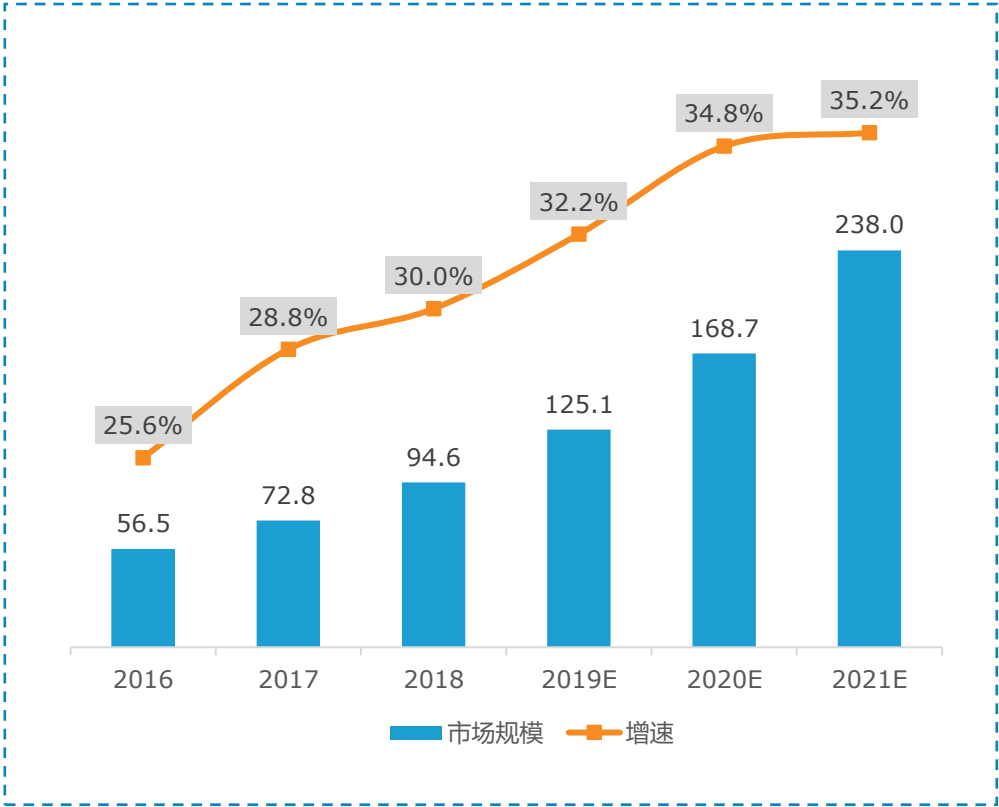
来源：国家信息安全漏洞共享平台、360、亿欧智库整理

制造业网络安全防护重点：工业互联网安全是制造业数字化的可靠保障

◆工业互联网安全是工业生产中的信息安全、功能安全与物理安全的统称，涉及工业互联网领域的各个环节，其核心任务是通过监测预警、应急响应、监测评估、攻防测试等手段确保工业互联网的稳定运行和健康发展。根据CCID数据，**2016- 2021年，工业互联网安全产业的市场规模复合增速达到30%以上。**

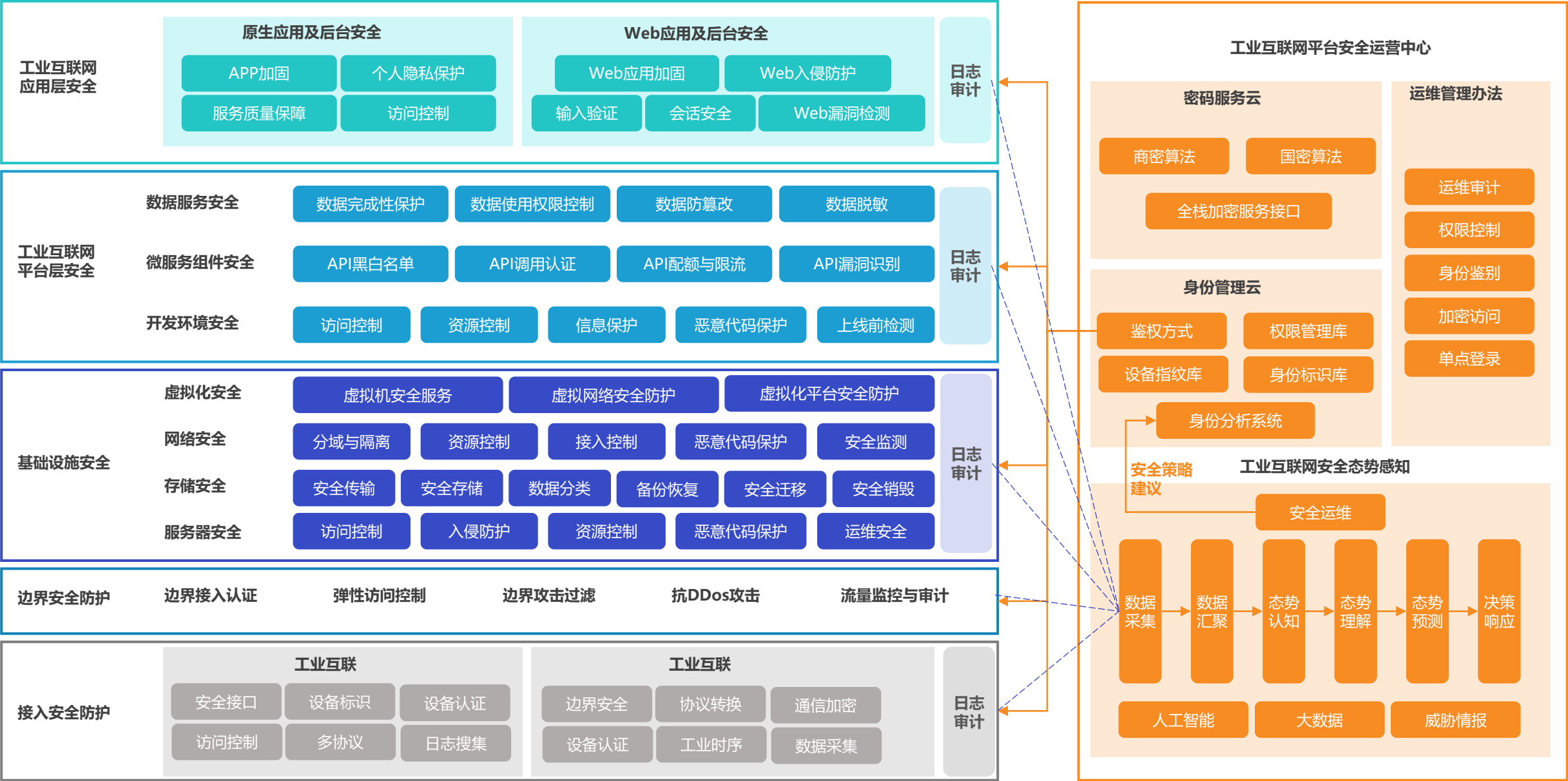


亿欧智库：2016-2021年中国工业互联网安全市场规模
(单位：亿元人民币)



来源：中国联通、CCID、'亿欧智库整理

工业互联网平台企业安全综合防护技术框架



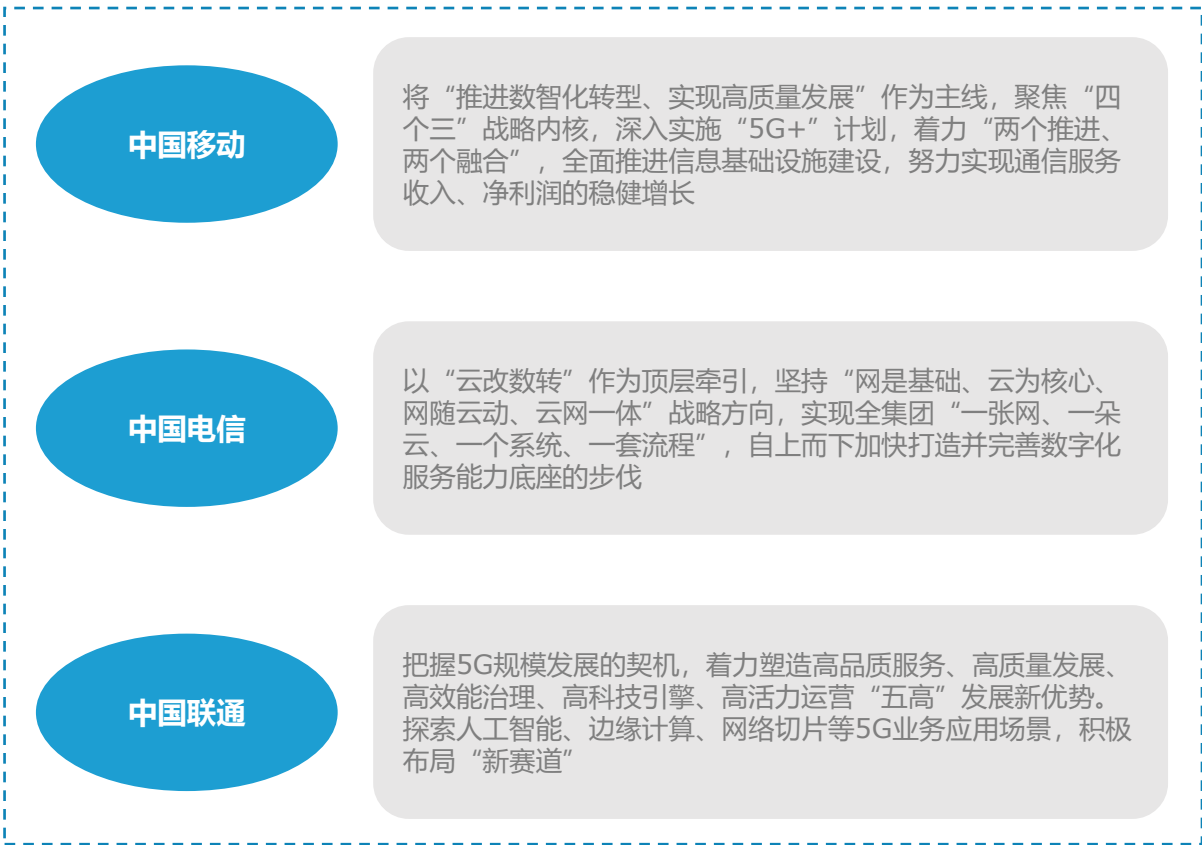
来源：工业互联网产业联盟，亿欧智库整理

运营商数字化转型背景：5G投入持续加大，发挥云网融合核心优势

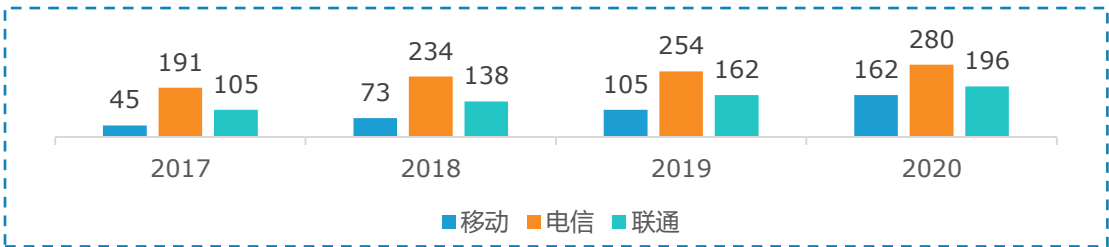
◆政企业务是5G时代运营商业务增长的主要引擎，2020年三大运营商的5G投入，较2019年均增长4-5倍。三大运营商正面向行业需求，发挥云网融合核心优势，服务产业数字化转型。

◆在传统业务市场饱和、流量红利日趋消失的背景下，**运营商不断加快数字化转型，云计算、IDC收入均水涨船高**。2017-2020年，中国电信IDC和云计算收入在三家运营商中位列第一。截至2019年，三大运营商共占中国IDC市场60.0%市场份额，其中电信最高占比30.6%。

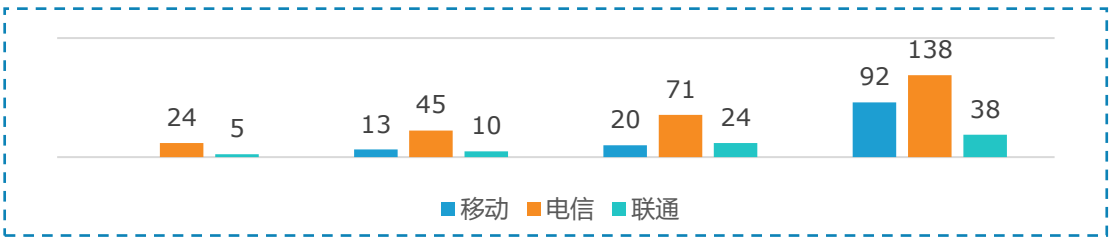
亿欧智库：2020年三大运营商数字化战略



亿欧智库：2017-2020年三大运营商IDC收入规模（单位：亿元人民币）



亿欧智库：2017-2020年三大运营商云计算收入规模（单位：亿元人民币）



亿欧智库：2019-2020年三大运营商5G资本开支（单位：亿元人民币）



来源：三大运营商公司年报、亿欧智库整理

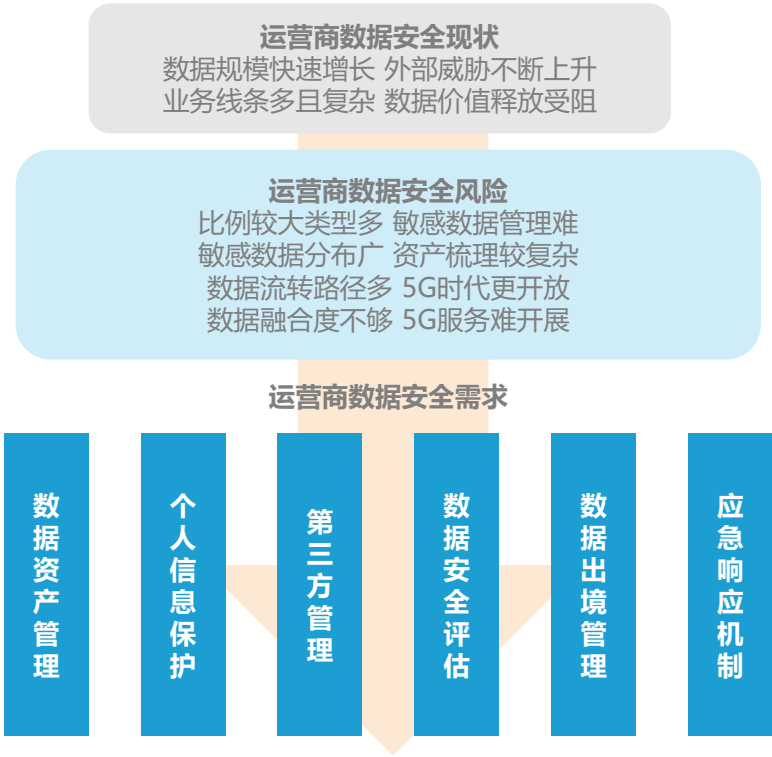
◆随着运营商数字化转型推进，海量数据的价值在流通、融合、共享中进一步被挖掘和提升，数据成为更多黑客的目标，近年来国内外电信行业数据安全事件频频发生。

◆截至2020年5月底，中国三家基础电信企业的移动电话用户数达15.9亿户。运营商大数据平台聚合了生产运营、网络承载、企业管理的数据，共1600多类，涉及3.8万属性，对外可输出通信、支付、社交、上网、身份、位置、时序、终端八大类核心数据能力。数据规模快速增长，如何保障数据安全，提升数据安全治理水平成为运营商的重要课题。

亿欧智库： 2020年全球电信行业网络安全事件

时间	事件经过
2020年10月	希腊最大的电信网络公司Cosmote发生重大数据泄露事件，大量用户的个人信息遭泄露
2020年7月	阿根廷电信1.8万台计算机感染勒索软件，黑客要价750万美元
2020年3月	美国电信巨头T-Mobile数据泄露导致用户个人财务信息曝光
2020年5月	日本电信巨头NTT遭黑客攻击，自卫队通信网络信息可能外泄
2020年5月	泰国最大移动运营商AIS云泄露83亿条互联网记录

亿欧智库： 运营商数据安全现状、风险及需求

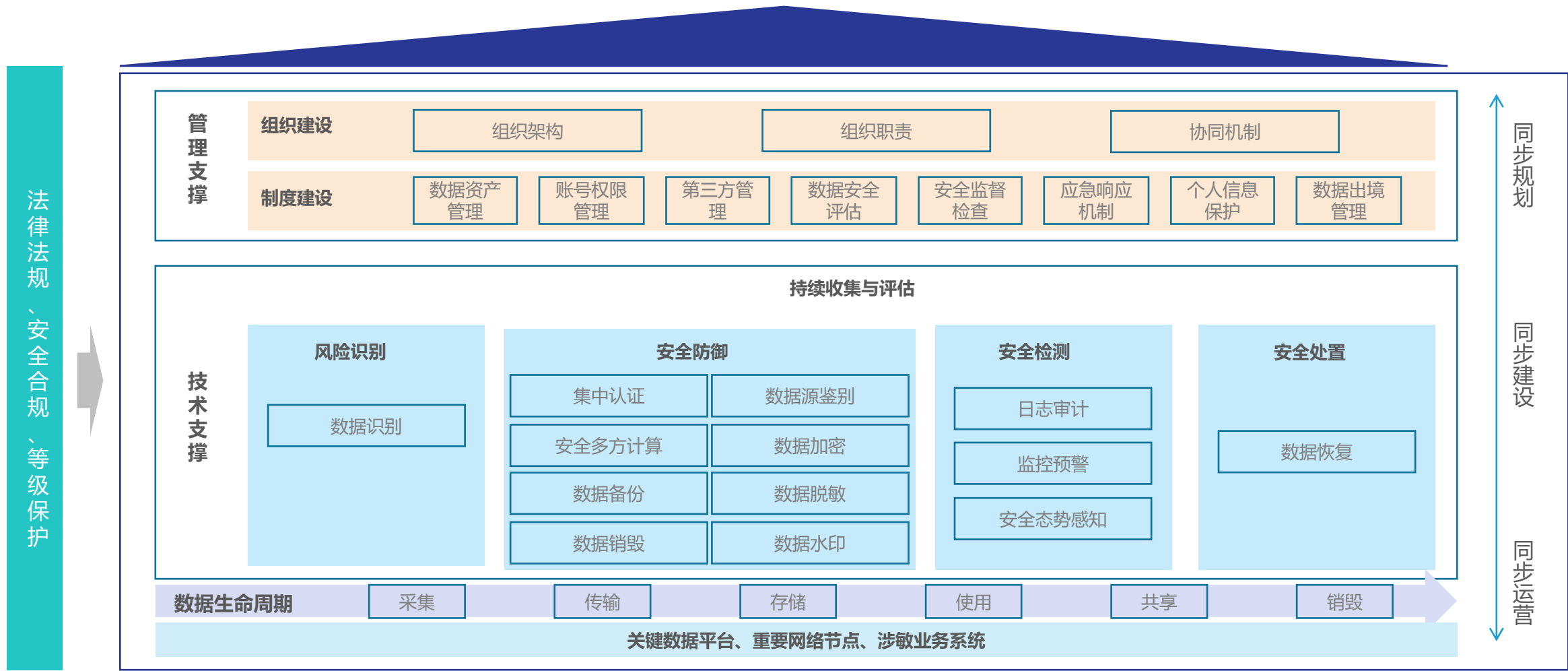


来源：《运营商数据安全白皮书》、亿欧智库整理

运营商网络安全重点：从管理和技术两方面构建防护体系

◆基于运营商的数据安全要求，以“**数据安全可管、可控、可视**”的防护目标。数据安全防护体系以关键数据平台、重点网络节点、涉敏业务系统作为底层应用系统，从管理和技术两方面构建防护体系。

亿欧智库：运营商数据安全防护体系

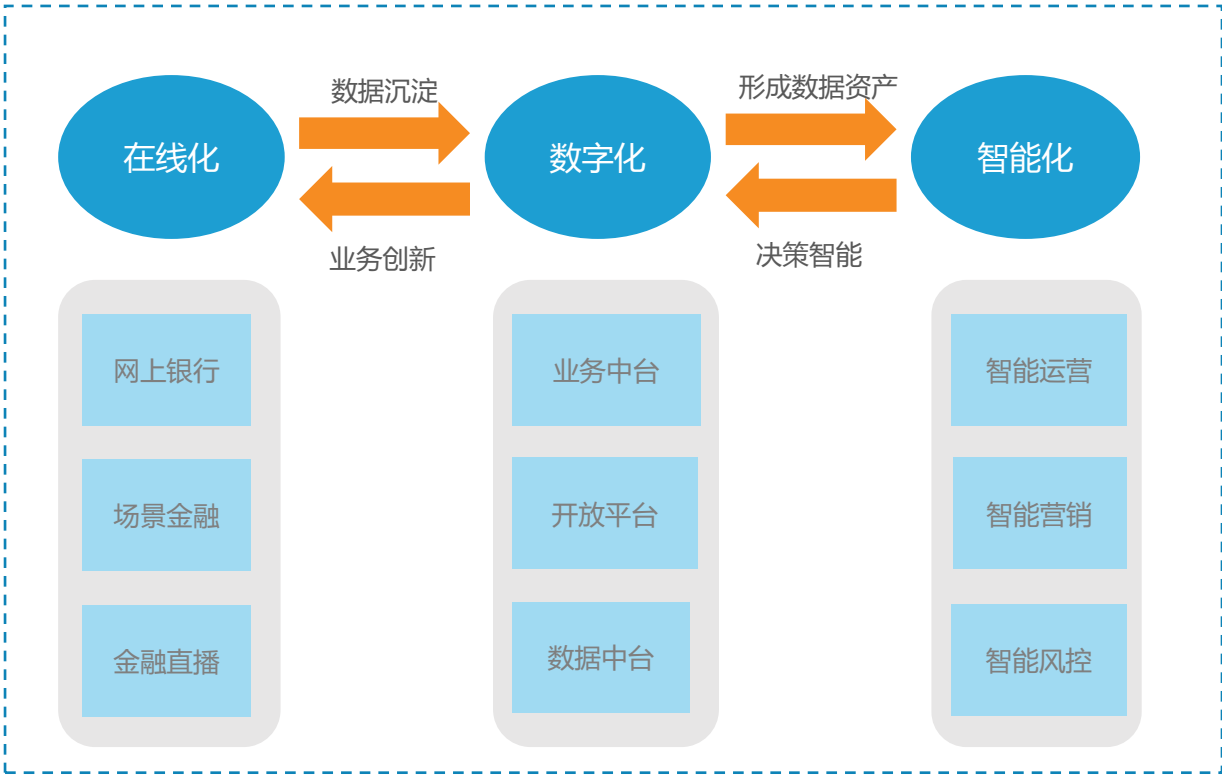


来源：《运营商数据安全白皮书》、亿欧智库整理

金融机构数字化转型背景：信息投入增长显著，重塑业务价值

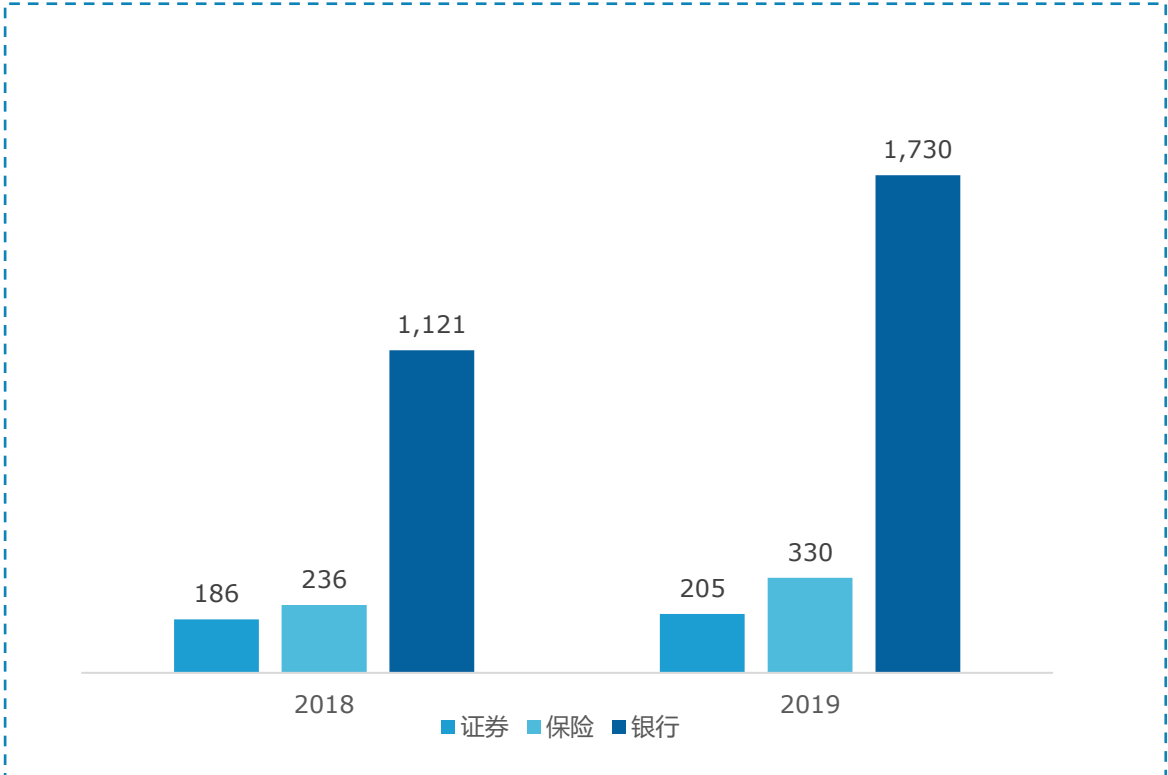
- ◆金融行业数字化指的是利用新兴技术，将交易数据沉淀，形成业务中台、开放平台、数据中台等，实现数据智能决策和智能交互，重塑金融机构价值。
- ◆随着金融服务线上化已成为习惯，客群行为呈现年轻化、互联网化、多元化，此外金融科技公司入局，传统金融核心业务面临挑战，传统金融机构服务模式开始重构，通过加大信息技术投入，提供不同维度、以及有针对性的服务，加强市场竞争力。

亿欧智库：金融数字化发展不同阶段与实现目标



来源：《未来金融白皮书》、亿欧智库整理

亿欧智库：2018-2019年中国证券行业、银行业、保险业信息技术投入对比
(单位：亿元人民币)



金融机构网络安全风险：攻击方式灵活多变，数据安全与隐私保护是核心

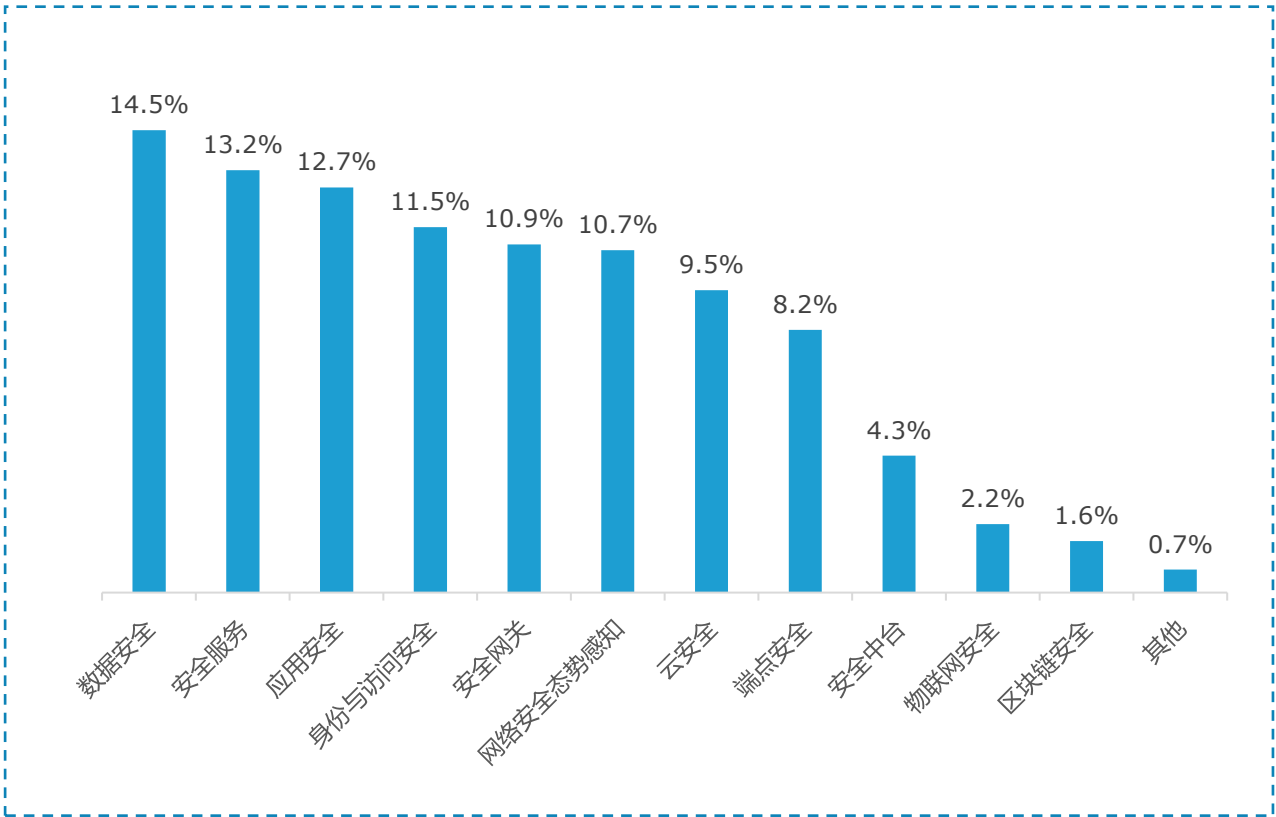
亿欧智库

- ◆《金融数据安全分级指南》、《个人金融信息保护技术规范》等标准规范密集出台，对数据安全和隐私保护赋予明确定义。根据《中国金融网络安全白皮书》，14.5%的金融机构将“数据安全”作为三年重点投入的第一选择。
- ◆相关检测报告显示，针对金融机构的网络攻击类型较多且方式灵活多变，以盗取资金、盗取敏感信息为目的，以SWIFT攻击、ATM攻击、信息泄露、恶意软件、网络诈骗、系统故障、勒索软件和DNS攻击等为主要攻击手段，金融机构经营发展受到严重影响，将造成巨大损失。

亿欧智库：金融机构安全现状、风险及需求



亿欧智库：2021-2023年主要金融机构网络安全主要投入领域




来源：《金融行业网络安全白皮书》、专家访谈、亿欧智库整理

- ◆2020年，中国人民银行发布了众多网络安全相关标准，用于指导和促进行业整体网络安全防范能力提升。
- ◆金融机构在选择网安厂商时，更为看重厂商技术能力、系统稳定性、服务质量三大因素。在技术应用方面，零信任网络架构备受关注，目前金融机构已在多个业务场景应用，尤其集中在传统安全方案普遍难以管控的场景，比如开发测试互联网出口的安全管控、内网跨区高危端口访问控制、零信任安全远程办公等。

亿欧智库：2020年中国人民银行所发布网络安全相关标准

时间	标准名称
2020年11月11日	《金融行业网络安全等级保护实施指引》 《金融行业网络安全等级保护测评指南》
2020年9月23日	《金融数据安全 数据安全分级指南》
2020年7月10日	《区块链技术应用 评估规则》
2020年7月10日	《证券期货软件测试指南 软件安全测试》
2020年7月10日	《证券期货业移动互联网应用程序安全规范》
2020年2月13日	《网上银行系统信息安全通用规范》
2020年2月5日	《金融分布式账本技术安全规范》
2020年2月13日	《个人金融信息保护技术规范》

亿欧智库：影响金融机构选择网安厂商的核心因素




技术能力

在产品正式部署前先进行测试，在测试过程中，判断产品是否能满足要求



系统稳定性

金融行业网络故障将会对客户造成极大损失，因此企业将十分看重安全产品稳定性



服务质量

金融行业发现安全问题后，需要及时响应，因此对安全厂商的服务质量要求很高

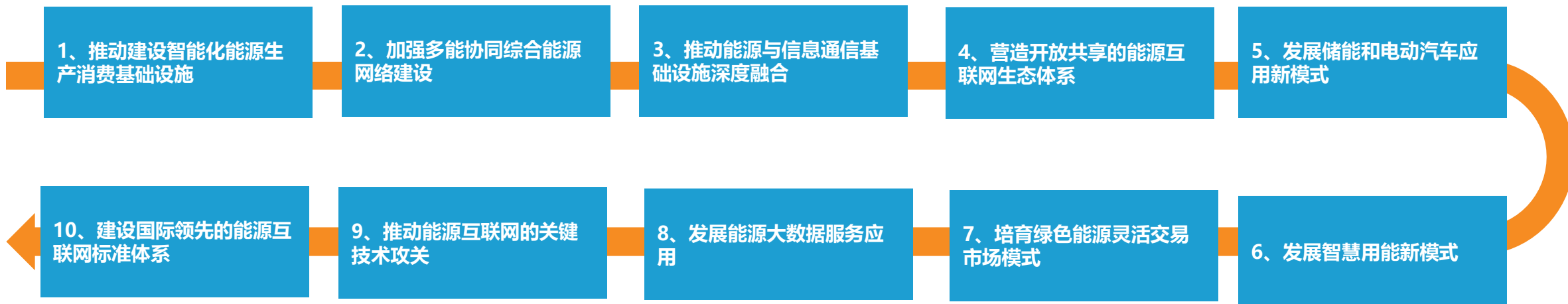
能源数字化转型背景：受政策倡导和效率提升的双重驱动

◆能源数字化转型的核心即使用新兴信息技术充分挖掘和利用能源全生命周期的数据价值。能源企业通过充分挖掘和利用经营过程的数据流价值优化自身的决策输出，从而提升能源生产、传输、交易与消费的运营效率，最终提升能源企业的经营效益以及能源行业的资源利用率与安全性。

◆2020年9月，国资委发布《关于加快推进国有企业数字化转型工作的通知》，提出要加快建设推广智慧电网、智慧管网、智能电站、智能油田、智能矿山等智能现场，着力提高集成调度、远程操作、智能运维水平，强化能源资产资源规划、建设和运营全周期运营管控能力，实现能源企业全业务链的协同创新、高效运营和价值提升。

◆2016年，国家能源局发布了《关于推进“互联网+”智慧能源发展的指导意见》，要求2019-2025年，着力推进能源互联网多元化、规模化发展，初步建成能源互联网产业体系，成为经济增长重要驱动力。

亿欧智库：“互联网+”智慧能源的十项重点任务

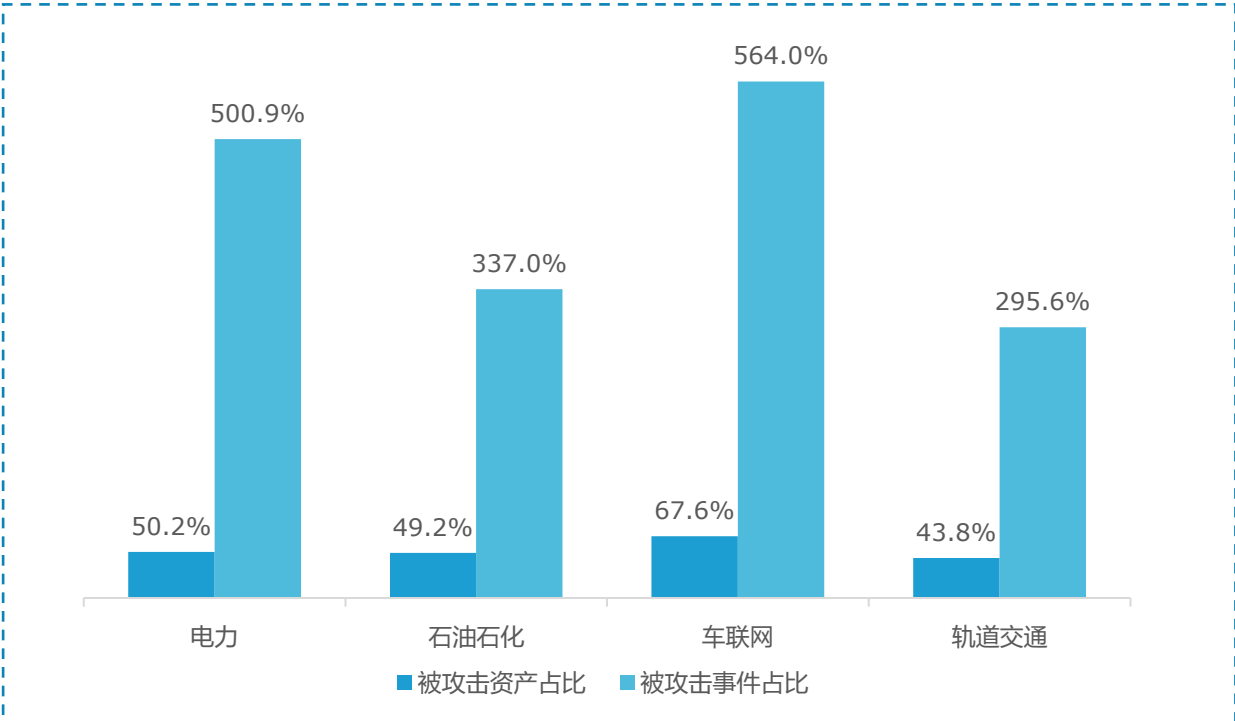


能源数字化转型安全风险：攻击频率高，危害程度深

◆工业4.0时代的到来，标志着能源行业正式进入互联网时代。与其它行业一样，迈向互联网即意味着风险的大量增加。能源行业的业务形态、服务对象、服务方式与其它行业不同，设备和系统具有专有性，因此给网络安全维护带来了巨大挑战。由于基础产业的特殊性，能源系统的宕机无疑将对宏观经济、社会发展带来巨大冲击，尤其在如今日趋复杂的国际局势下，来自能源行业的网络安全威胁更比任何时候都显得更加严峻。

◆国家关键基础设施安全应急响应中心2021年第四次监测，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）。监测发现，遭受攻击的资产有1240个，涉及攻击事件11490起。

亿欧智库：2021年国家关键基础设施安全应急响应中心重点行业资产及攻击事件分布



备注：被攻击资产占比=该行业被攻击资产数/该行业监测资产数；被攻击事件占比=该行业被攻击事件数/该行业监测资产数
来源：国家关键基础设施安全应急响应中心、亿欧智库整理

亿欧智库：2020年全球重大能源网络安全事件

时间	事件
2020年1月	欧洲能源部门服务器被植入 PupyRAT 后门
2020年2月	美国某天然气运营商遭勒索攻击被迫关闭
2020年4月	Agent Tesla 间谍软件被用于针对能源行业的鱼叉攻击
2020年7月	伊朗纳坦兹核设施起火可能是人为破坏
2020年7月	葡萄牙能源巨头 EDPR NA 遭勒索并且影响母公司 EDP
2020年7月	巴西电力公司 Light SA 遭 Sodinokibi 勒索
2020年9月	Netwalker 勒索软件袭击了巴基斯坦主要的电力供应商 K-Electric
2020年10月	跨国能源公司 Enel 集团遭到勒索软件攻击

能源网络安全防护重点：一体化运营打造电网网络安全保障体系



1

强化公司安全管控能力

落实国家、行业网络安全政策要求，优化管控机制，明确安全管理任务，提升风险预警及应急处置能力。

2

完善健全标准规范支撑体系

研究国家、行业标准规范，借鉴国外先进标准为我所用。

3

构建闭环的一体化安全运营体系

安全预警监测平台为技术载体，实现人员、技术、流程的整合，持续输出安全成效。

4

健全安全组织机构

明确组织职责、优化协同机制、完善人员管理、加强人员培养、提升人员安全意识。

5

完善技术防护体系，实现安全防护能力全面覆盖

以安全即服务思想构建安全基础设施，提供通用安全服务能力，有效支撑安全运营。

数据来源：奇安信、国家电网、亿欧智库整理

典型案例

Companies list

360：政企数字安全先行者与引导者

- ◆ 成立于2005年的360是我国网络安全行业的资深玩家。除了在C端网安产品领域拥有巨大影响力之外，**2019年9月，360集团对外宣布，公司政企安全战略进入3.0时代，将执行以“共建、分享、赋能、投资”的发展模式，构建安全大生态。**
- ◆ 凭借近20年的探索和积累，360已经积累了网络安全领域雄厚的技术实力和丰富的行业经验。
- ◆ 在数字化转型和大安全时代的挑战下，360再次加速升级政企网络安全策略，依托于大数据积累、行业项目经验和精英团队的储备，**360构建了面向未来的数字安全能力体系。**

亿欧智库：360网络安全领域的技术实力和行业积累

- **20年**的安全思考
- **200亿**的安全投入
- **200人**的安全精英团队
- **3800人**的安全专家团队
- **2EB**的安全大数据
- **全国200个**物理机房
- **全球独有300亿**样本
- **捕获46个**APT组织

数据来源：360、亿欧智库整理

亿欧智库：360面向未来的数字安全能力体系



亿欧智库：360七大安全框架



苏州吴中大数据管理局安全运营项目

- 加强吴中区电子政务安全运营建设
- 提升城市网络安全抗风险能力
- 打造网络安全全国创新应用示范点
- 打造安全、可信的电子政务网络环境

项目背景

- 360政企安全集团中标苏州吴中大数据管理局重大项目，围绕数字政府基础设施的网络安全建设展开合作，共同构建数字政府安全运营服务新体系，高效助力苏州吴中地区应对数字时代高级威胁攻击，整体提升城市网络空间安全对抗能力。

- 业务挑战**
- 缺乏整体安全态势监测手段
 - 缺乏安全事件闭环管理流程
 - 缺乏安全服务保障体系

解决方案

项目遵从“三同步”原则，实行同步设计、同步建设、同步运营，规划设计了安全运营体系、安全验证体系、安全度量体系，并分别建设：

政务网络安全大数据分析底座

聚合电子政务云端边安全大数据，借助360的威胁分析能力，增强网络安全感知和应急能力。

安全运营管理中心

组建安全运营专家团队，建立日常安全运营管理制度，提供应急调度管理机制，综合提升电子政务网络安全应急能力。

安全运营服务流程

制定安全运营流程和执行预案，在保障业务安全的前提下，形成威胁预测、威胁防护、持续监测、响应处置的闭环安全运营管理

郑州人民医院安全运营中心项目

- 完善安全运营体系
- 保障医疗数据安全
- 为体现医疗数据价值提供基石
- 建立医疗行业数据安全标杆

项目背景

- 360政企安全集团建立郑州市人民医院安全大脑，再以安全服务赋能医院安全基础设施，通过打造“合法合规+持续运营+有效治理”的业务安全一站式运营模式，实现郑州人民医院数据安全治理，加强网络安全防御体系建设，保证各类业务稳定运行。

- 业务挑战**
- 缺少外网与内网的数据缓冲区域
 - 缺乏统一的重要数据授权和细粒度访问控制
 - 缺少运营平台和自动化流程的支撑

解决方案

建设数据安全运营管理体系

打通医院现有不同信息系统间的数据流通壁垒，提供统一的数据安全交换和协同交互的平台。

建设安全运营基础设施

提升安全运营和安全管理能力，加强网络安全防御体系建设保证各类业务稳定运行。

落实安全运营制度

依托国家、行业相关标准，持续改善安全运营机制，实现信息系统符合等保、电子病历、医院互连互通等相关标准。

医院智慧服务评级

通过评估医院智慧服务等级，指导医院以问题和需求为导向持续加强信息化建设、提供智慧服务。

- ◆ 安恒信息于2007年成立于浙江杭州，并在2019年成功上市科创板。自成立以来，安恒信息一直专注于网络信息安全领域，秉承着“助力安全中国，助推数字经济”的企业使命，深耕政企客户，**具备国家级网络安全保障实力**。
- ◆ 在数字化转型和大安全时代的挑战和机遇下，安恒信息持续优化产品结构，加大研发投入，在云计算、大数据、物联网、智慧城市、工业互联网等新兴赛道全面发力。**构建了覆盖网络信息安全生命周期的产品体系**。

亿欧智库：安恒信息全生命周期安全服务业务概览



亿欧智库：安恒信息技术优势



数据来源：安恒信息、亿欧智库整理

甘肃省公安厅天鉴关键信息基础设施安全防护管理平台项目

亿欧智库：天鉴平台架构

项目需求

精准掌握区域内网络威胁活动情况

平台权限下放各级，按需监测

有效提升网安通报时效性、准确性和权威性

建立各级公安通报联动机制

业务挑战

缺乏网络安全监测预警和态势感知能力

缺乏事件应急响应机制和调查技术

缺乏数据收集以及追踪溯源能力

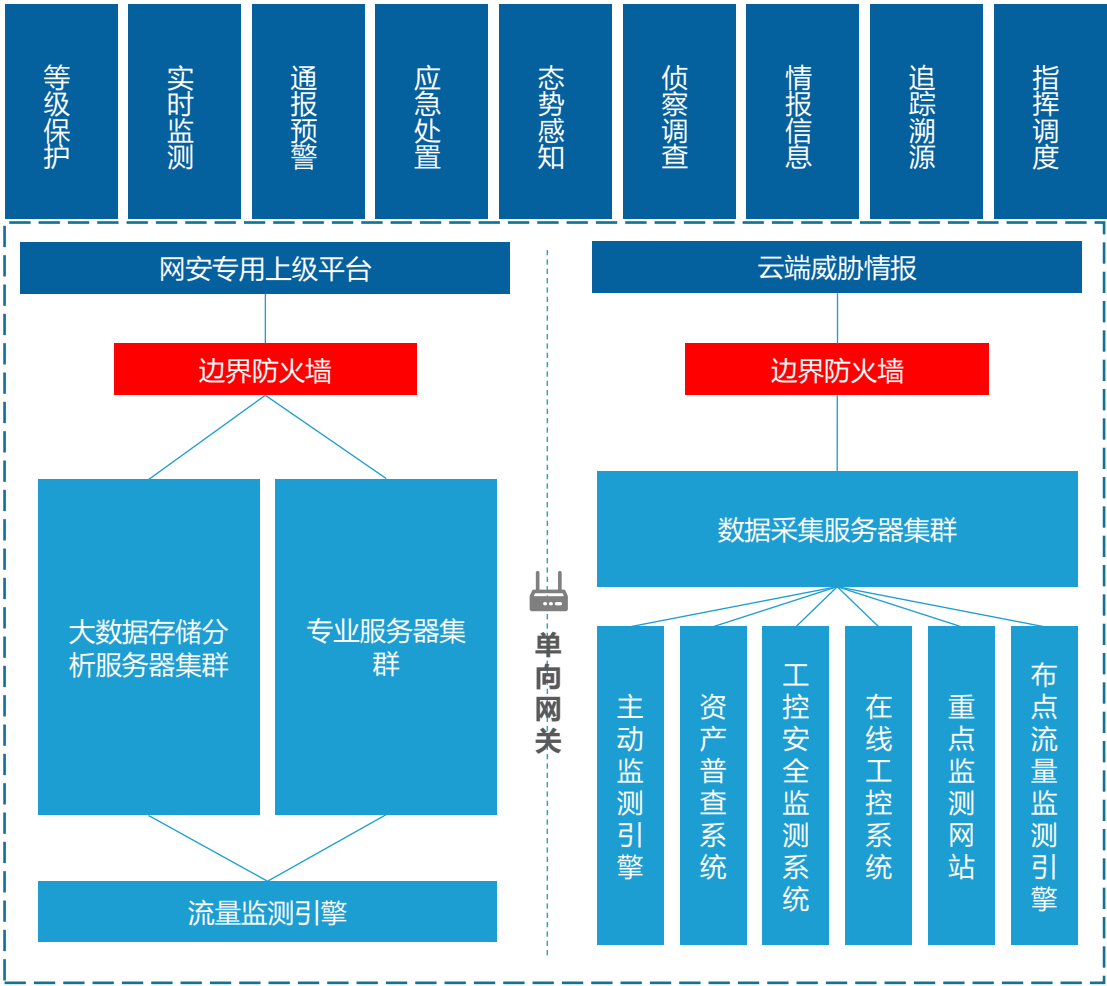
解决方案

在公安部针对网络安全监测和态势感知系统的指导要求下，为甘肃省公安厅建设的关键信息基础设施安全防护管理平台分别包括：

- ◆ 网络安全监测预警和态势感知系统：实现对等级保护检查的曾理，建立7x24小时的监测体系于全天候全方位网络安全态势感知分析能力。
- ◆ 应急响应机制与调查技术：提供有效的应急防护业务指导以及技术支撑，并在事后提供一系列技术手段和行政办理管理流程与案件线索检索手段。
- ◆ 第三方情报数据收集，开展追踪溯源：从网络空间中搜集数据流量并加以分析，对网络威胁事件根据数据流转路线进行追踪溯源，为公安办案、破案提供有力的技术支撑手段。

平台建成后，形成了区域范围的网络监测与预警能力，快速告警和响应机制。

数据来源：安恒信息、亿欧智库整理



- ◆ 山石网科成立于2007年，作为中国网络安全行业基础创新领导厂商，于2019年9月，以首批科创板上市网络安全公司身份登陆科创板。
- ◆ 自成立以来，山石网研发投入多年占比超过27%，并掌握21项自主研发核心技术。形成了具备“**全息、量化、智能、协同**”四大技术特点的涉及边界安全、云安全、数据安全、业务安全、内网安全、智能安全运营、安全服务、安全运维等八大类产品服务，50余个行业和场景的完整解决方案，累计服务超20000家用户。

亿欧智库：山石网科安全产品体系



数据来源：山石网科、亿欧智库整理

项目背景

山石网科助力甘肃电信建设可信云资源池，构建云内业务安全。其产品山石云·格完美解决甘肃电信在云内流量可视可控，以及云内安全方面的需求，得到了甘肃电信的认可，并在全国区域内得到进一步的推广。

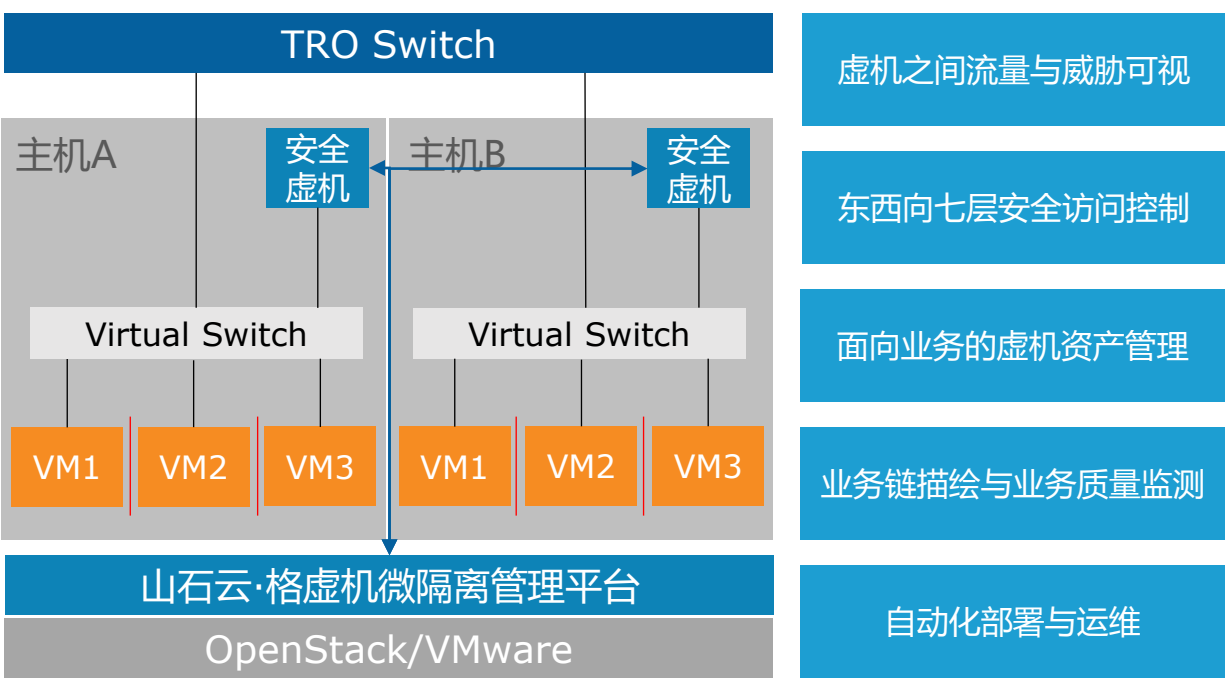
业务挑战

- 电信IDC虚拟化数据中心规模大，亟需云内流量可视可控方案
- 缺乏网络侧微隔离防护，以便形成整体立体防护方案
- 云内资源池集群大，易受挖矿病毒、木马攻击，且威胁易横向扩散
- 难以察觉云内攻击行为，发生重大事故后，溯源、响应、取证困难
- 现有IT人员缺乏应对云内业务系统运维运营能力

- ◆ 山石网科虚拟化防护产品-山石云·格部署在甘肃电信虚拟化数据中心内（13个集群），其内置安全服务结合亚信的终端杀毒产品形成云资源池内网络微隔离防护+本地查杀的整套立体防护方案，对云资源池内的电信云化业务系统进行全面安全防护，总计防护2000+业务虚拟机。
- ◆ 采用山石云·格的透视镜、SPM、策略助手、策略分组等功能，实现资源池内复杂的业务交互关系可视、梳理及安全策略收敛。
- ◆ 安全服务适应云计算特性，可根据业务需求进行弹性伸缩扩展，满足快速上线需求。
- ◆ 同时山石云·格无代理防护方案与VMware的良好兼容性、可靠性以及后期战略性的支撑华为云平台赢得客户双重认可。

数据来源：山石网科、亿欧智库整理

亿欧智库：山石云·格虚拟机微隔离架构



亿欧智库：微隔离实施过程——五步法



企业榜单

Companies list



2021年中国政企数字化网络安全TOP50企业榜单



SANGFOR
深信服科技



新一代网络安全领军者



2021年中国政企数字化网络安全TOP50企业榜单



◆ 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：



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

◆ 版权声明：

本报告所采用的数据均来自合规渠道，分析逻辑基于智库的专业理解，清晰准确地反映了作者的研究观点。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。本报告的信息来源于已公开的资料，亿欧智库对该等信息的准确性、完整性或可靠性作尽可能的追求但不作任何保证。本报告所载的资料、意见及推测仅反映亿欧智库于发布本报告当日之前的判断，在不同时期，亿欧智库可发出与本报告所载资料、意见及推测不一致的报告。亿欧智库不保证本报告所含信息保持在最新状态。同时，亿欧智库对本报告所含信息可在不发出通知的情形下做出修改，读者可自行关注相应的更新或修改。

本报告版权归属于亿欧智库，欢迎因研究需要引用本报告内容，引用时需注明出处为“亿欧智库”。对于未注明来源的引用、盗用、篡改以及其他侵犯亿欧智库著作权的商业行为，亿欧智库将保留追究其法律责任的权利。

◆ 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。

◆ 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。

◆ 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

查看更多研究报告请访问亿欧网
www.iyiou.com

- 更有超多垂直领域研究报告免费下载 -



扫码添加小助手
加入行业交流群

