中国平安 PINGAN
金融·科技

计算机行业深度报告

证券研究报告

网络安全：新时代、新挑战、新机遇

2021年10月20日

证券分析师

付强 投资咨询资格编号：S1060520070001 FUQIANG021@pingan.com.cn
闫磊 投资咨询资格编号：S1060517070006 YANLEI511@pingan.com.cn

计算机行业评级：强于大市（维持）

投资要点

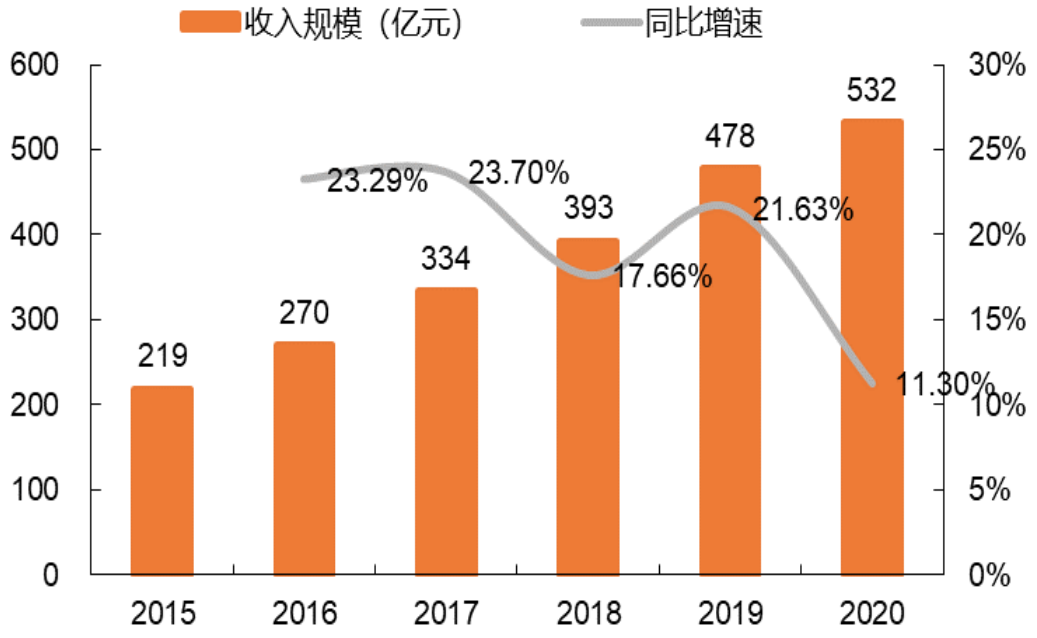
- **现状：安全行业正在恢复，竞争格局在改善。**受到疫情影响，2020年国内网络安全行业增速出现明显下滑，尤其是安全硬件增速下降较为显著。从客户结构上看，政府、金融、运营商、教育等行业是安全厂商收入的主要来源；从客户数量看，医疗卫生、教育、政府和金融业的客户数量实现较高增长。竞争格局分散一直是行业发展面临的问题，但近年来逐步改善，CR1、CR4和CR8均较2020年提升，其中CR8已经超过40%。2021年以来，国内数字化转型提速，合规要求也在趋严，龙头企业收入多数都实现了较快增长，预计行业集中度将进一步提升。
- **挑战：数字化转型提速，但安全形势更为复杂。**当前，数字经济发展较为快速，数据量增长迅猛。但是，网络犯罪正在侵蚀数字经济成果。据Cybersecurity Ventures预测数据显示，2021年全球因为网络犯罪带来的损失将高达6万亿美元，该数字超越了中国2020年数字经济体量，也高于日本2020年的经济规模；到2025年，该机构预测全球由于网络犯罪带来的损失将达到10.5万亿美元。如此规模的财富破坏和非法转移，必须予以重视并阻止。当前，网络安全主要面临着来自三个方面的挑战：第一，外部攻击出现新的变化，勒索病毒攻击更为频繁且破坏力更强，供应链攻击等新手段也在被APT组织持续利用，DDoS攻击手法更为复杂多样，新场景如云平台、车联网、工控平台受到威胁空前；第二，来自组织内部的攻击增多，且难以防护；第三，合规要求明显趋严，《数据安全法》《个人信息保护法》《关键信息基础设施保护条例》等法律法规正在落地，行业来自合规方面的压力增大。
- **机遇：网安与数字化融合加速，中高速增长可期。**从整个网络安全发展主脉络来看，无论是“攻防”还是“合规”，最核心的逻辑还是信息化、数字化发展到足够水平之后，安全才更重要。2021年以来，国内对数字经济的发展特别关注，产业数字化、数字产业化、数字化治理产业规模快速扩大，新威胁和新挑战相伴而生，安全同信息化、同业务在深度融合，行业进入新时代。预计到2023年，国内网络安全产业规模有望达到861亿元，2021-2023年收入平均增速将达到17.4%，其中软件增速将超过20%。从技术趋势看，安全云化、服务化将提速，零信任、容器安全、SASE（安全访问服务边缘）有望在未来2-5年内走向成熟，隐私计算应用范围也将扩大，车联网安全解决方案也将逐步成型。
- **投资建议：**在我国数字化、智能化发展的大背景下，我国网络安全行业也面临着新变革。线上化、云化提速让安全边界变得更为模糊；工业互联网和智能制造的发展也使得工控领域的安全风险持续暴露；产业数字化带来的数据资产快速积累，安全防护的重心也在向数据安全迁移。同时，国内网络安全监管进一步趋严，网络安全法律法规与行业标准正在密集出台，尤其是对新安全领域的防护，如数据安全、车联网安全等，要求更为严格。国内网络安全行业也正在顺应变化，加快技术研发投入，发力新安全领域，高景气发展将持续。强烈推荐**启明星辰**，推荐**深信服、安恒信息和绿盟科技**。同时，重点关注市场竞争加剧的风险、技术风险和下游客户IT支出不及预期的风险。

目 录 CONTENTS

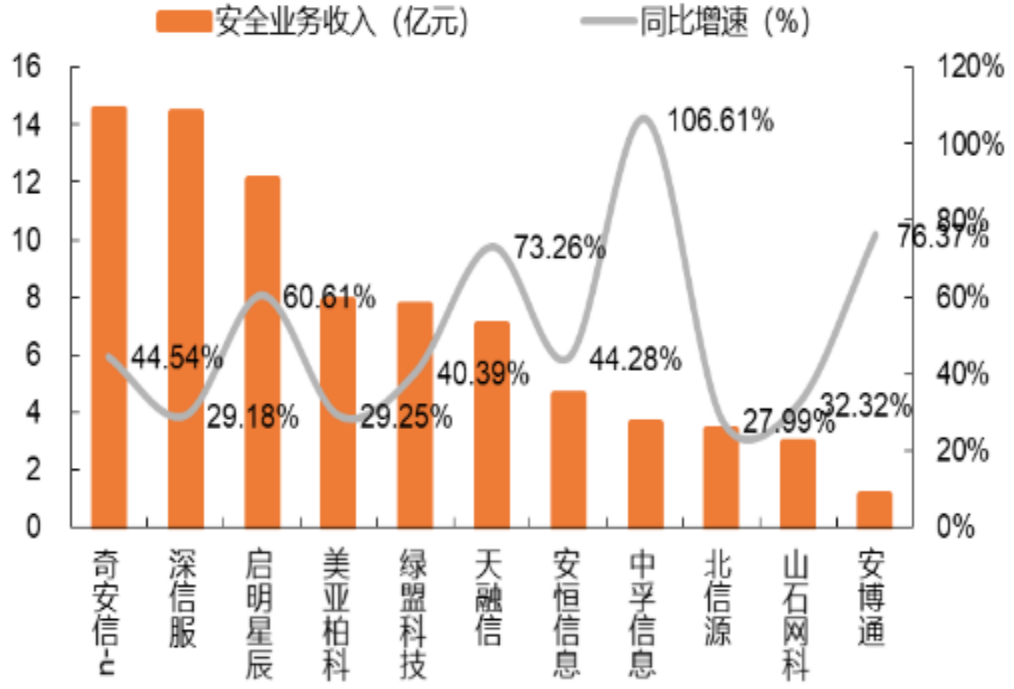
现状|行业恢复较为明显，21H1主要企业收入增长快速

- 2020年，受到疫情影响，整个网络安全行业增速出现明显下滑。中国网络安全产业联盟（简称CCIA，下同）调研数据显示，2020年行业实现收入532亿元，同比仅增长11.30%，较上年同期下降10.33个百分点。虽然2020年传统网络安全硬件表现不佳，但是安全软件和服务则为全年增长仍提供了支撑。
- 2021年以来，由于疫情负面因素基本消失，网络安全行业表现出较好增长势头，主要上市企业网络安全业务收入均实现了较快增长。

2015-2020年我国网络安全行业收入规模及增速



2021年上半年我国主要网安企业收入及增速

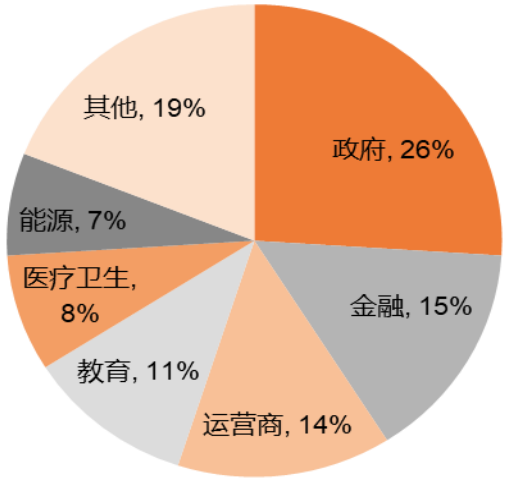


数据来源：中国网络安全产业联盟（CCIA）、数说安全、平安证券研究所

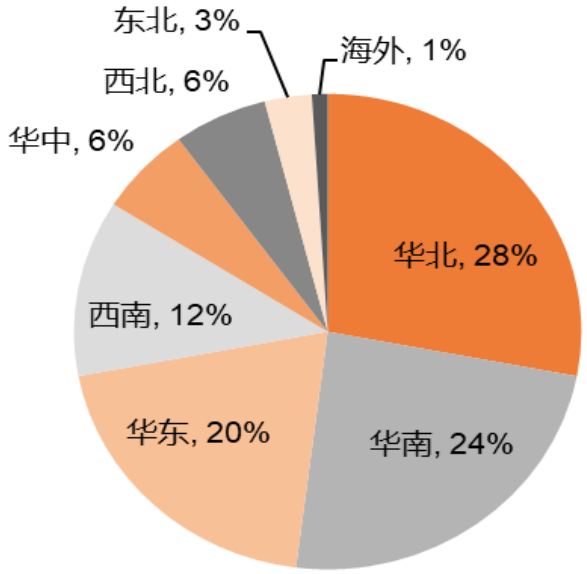
现状|政府、金融、运营商及教育等行业是收入主要来源

- 政府、金融、运营商、教育等行业网络安全市场规模占比均在10%以上，合计占到整个市场的66%；医疗卫生、能源网络安全收入规模占比分别为8%和7%。未来，随着数据安全、关键基础设施保护相关政策的落实，这些重点行业信息化投入中，安全占比还将提升，增长潜力依然存在。
- 华北、华南以及华东地区是网安行业主要收入的来源，但2020年各地对安全投入的力度都有不同程度的提升，西南地区尤其是四川和重庆收入规模扩大比较明显。

2020年我国网络安全收入结构（按行业）



2020年我国网络安全收入结构（按地区）

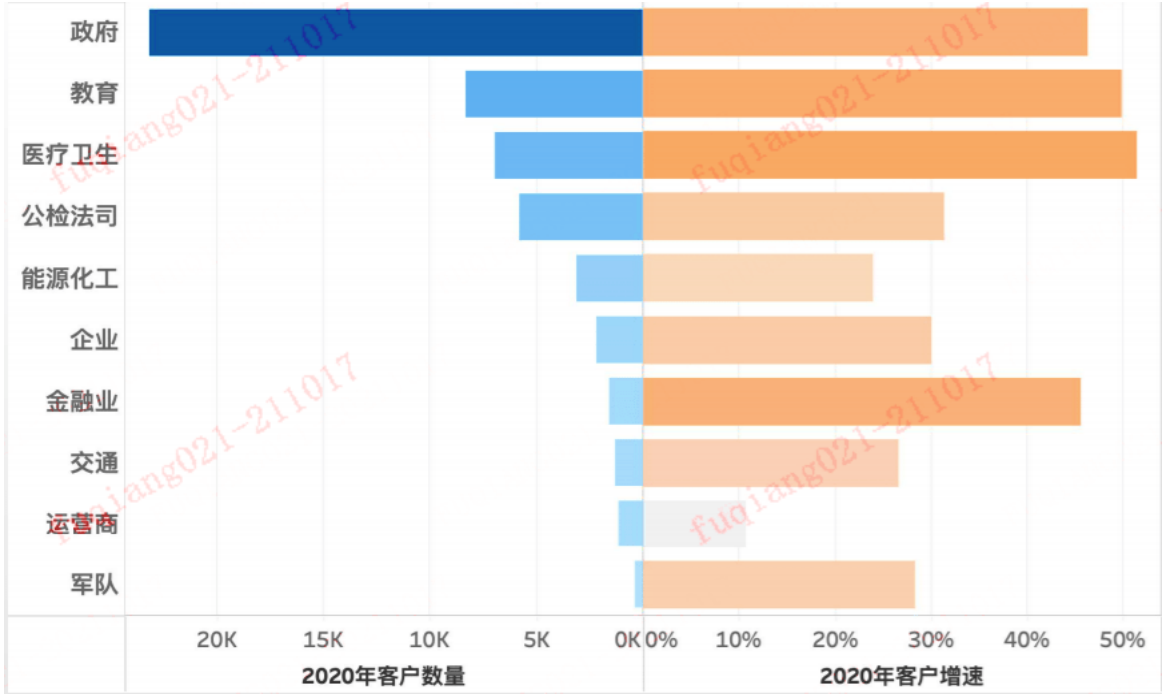


数据来源：中国网络安全产业联盟（CCIA）、数说安全、平安证券研究所

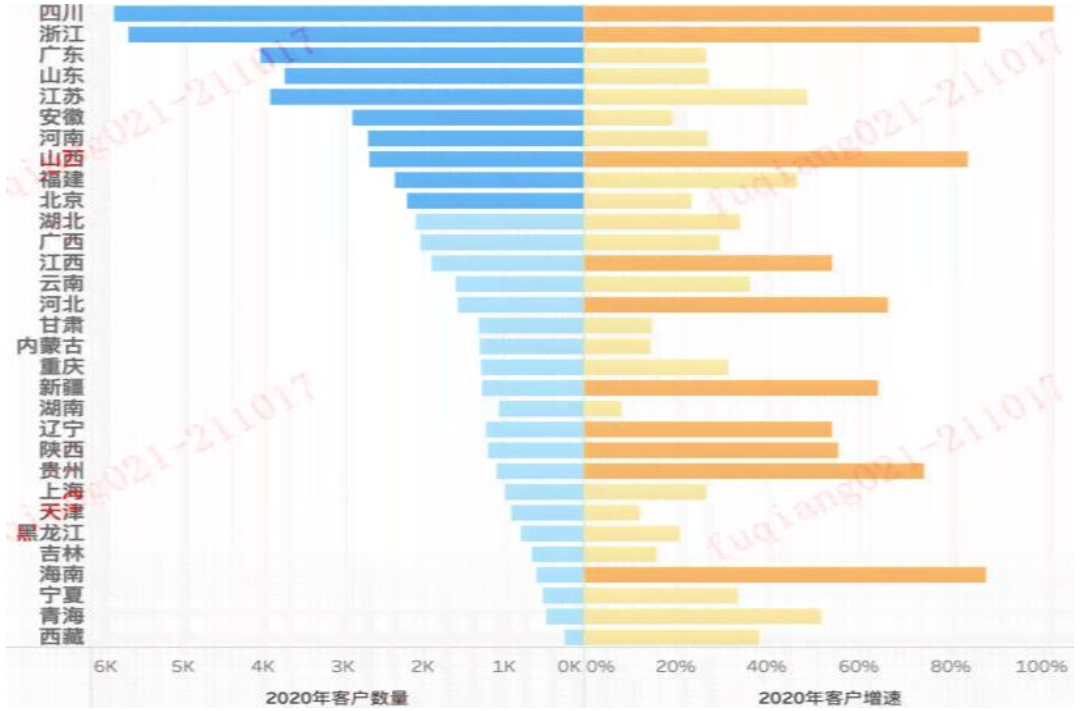
现状|医疗、教育、政府和金融客户数量保持较快增长

- 政府、教育、医疗卫生、公检法司和能源化工行业是我国网络安全行业客户最为集中的领域。CCIA数据显示，2020年，全国网安客户数量超过9万家，其中新增客户3万家。前述5大行业客户数量占据了全国84%的份额，其中政府客户数量最多，占据了43%的份额。从增速上看，2020年，医疗卫生、教育、政府和金融业的客户数量保持较高增长。
- 主要客户集中在京津冀、长三角和珠三角地区，但近年来中西部地区开始关注网络安全建设，如行业客户相对较少的江西、云南、贵州等地区，2020年客户数量增长较快，客户数量比较高的浙江和四川，2020年客户数量增长也较快。

国内网络安全行业客户分布及增速（家）



国内网络安全行业客户分布及增速（家）

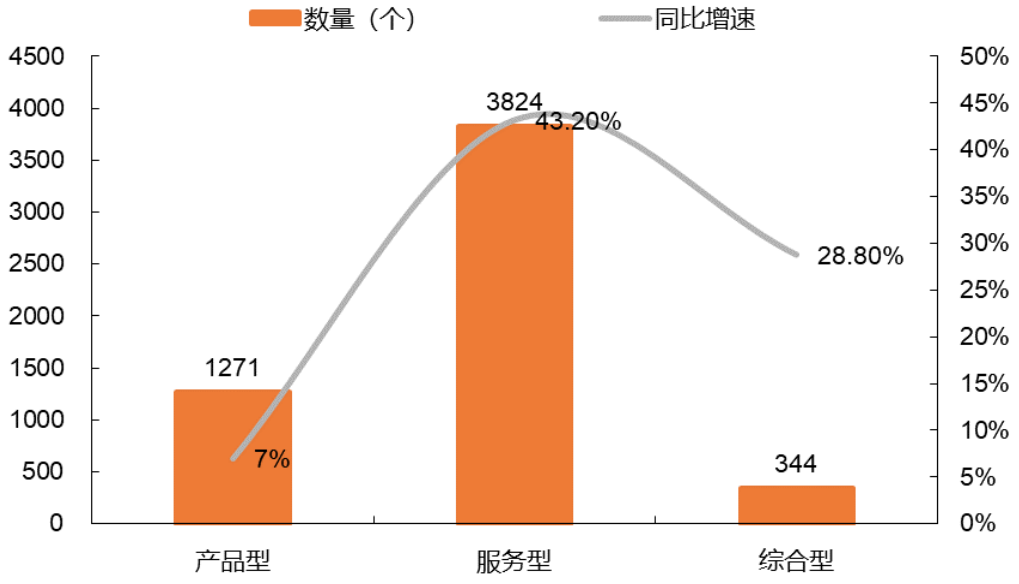


数据来源：中国网络安全产业联盟（CCIA）、数说安全、平安证券研究所

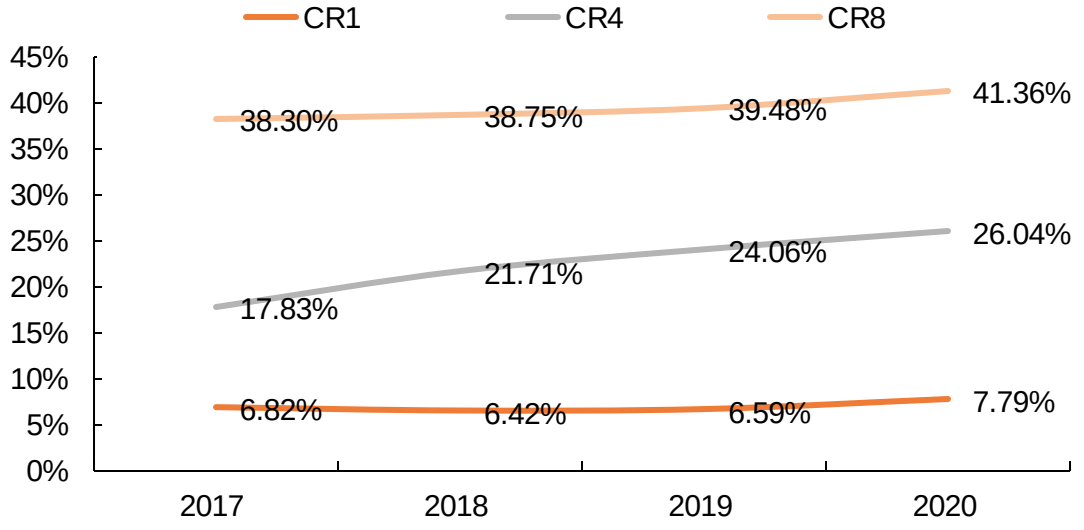
现状|市场集中度小幅提升，竞争格局持续在改善

- 截至2021年上半年，我国共有4751家公司开展网络安全业务， 相比上一年增长 23.1%。其中，产品型和服务型企业分别为1271家和3824家，综合型企业有344家（产品型和服务型类别中也均包含该类企业）。其中，北京、广东和上海企业数量居前，分别为1080家、730家和323家。
- 整体市场集中度小幅提升。2020年我国网络安全市场CR1为7.79%，CR4为26.04%，CR8为41.36%，均高于2019年。当网络安全市场进入稳健增长阶段后，头部企业在规模和资源上拥有明显优势。随着时间推移，头部企业拥有的市场份额会逐渐扩大，预计未来我国网络安全市场集中度将持续提升。

2021年上半年末国内网络安全企业数量



国内网络安全行业市场集中度变化



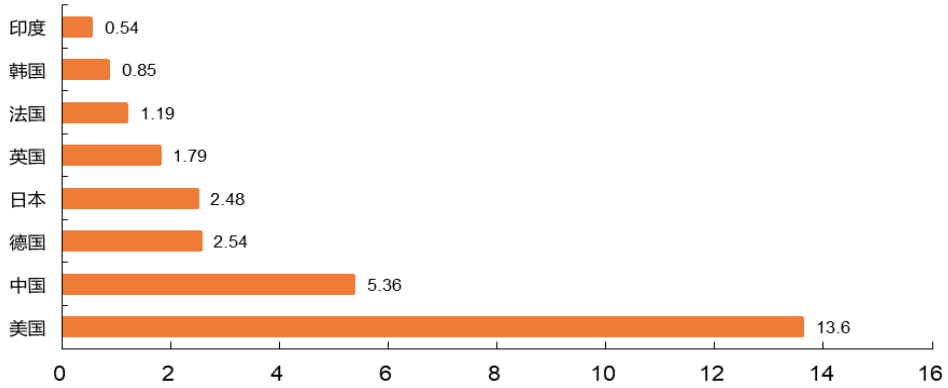
数据来源：中国网络安全产业联盟（CCIA）、数说安全、平安证券研究所

目 录 CONTENTS

挑战|数字经济发展快速，数据产生和处理量将爆发

- **数字经济已经成为各国竞相角力的领域，成长迅速。**2020年全球数字经济规模达到32.6万亿美元，占全球经济的比重达到43.7%，同比增长3.0%，而同期主要经济体经济都是负增长。其中，我国数字经济体量达到5.36万亿美元，仍稳居市场第二位。
- **信息的数字化成本收益比非常高，各类应用也都在加快数据的产生、处理、流通、使用和存储，数据也成为经济发展的要素之一。**据IDC数据显示，全球产生和存储的数据量将从2018年的33ZB（1ZB=1万亿GB）的上升至2025年的175ZB。线上用户数量，软件开发者和需要保护的代码量持续上涨，连接的数量也将从2020年的330亿上升到2025年的750亿。

2020年主要国家数字经济规模对比（万亿美元）



生产要素构成

全球主要数字化指标和预测

75亿
人在线上并产生数据，2030年

35亿
智能手机用户，超过45%的渗透率（2020）

1900万
软件开发者（2019），预计到2030年将达到4500万

3380亿
行需要保护的新软件代码量（2025）

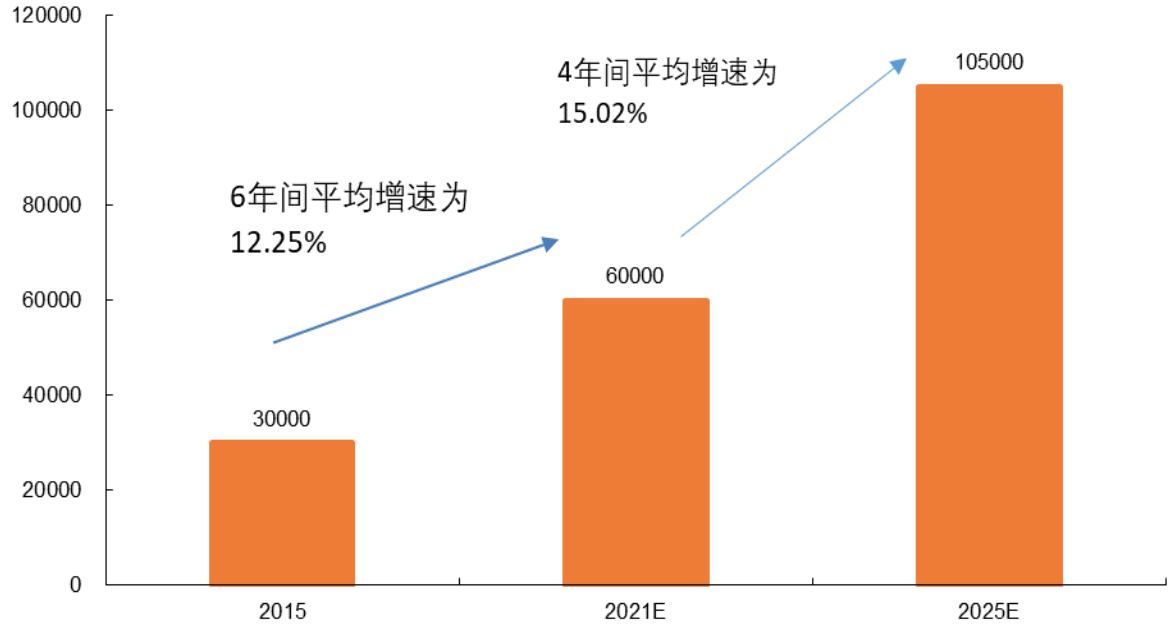
310亿
连接的设备（2020），预计到2025年将有750亿 IOT设备接入

数据来源：信通院、Cybersecurity Ventures、平安证券研究所

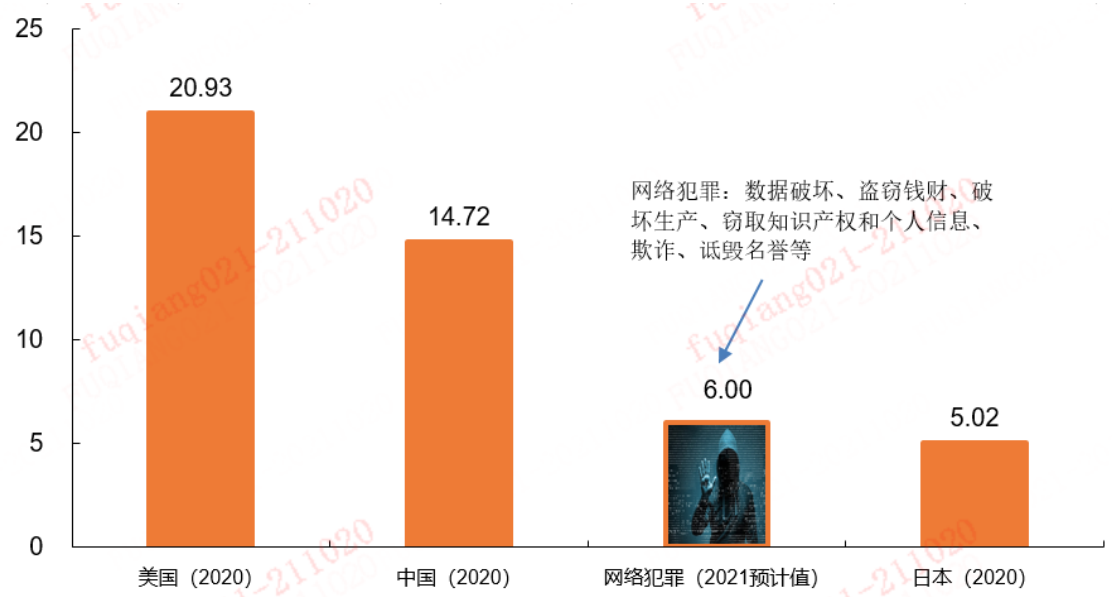
挑战|网络犯罪在偷窃和侵蚀数字经济成果，破坏力巨大

- **网络犯罪带来的经济损失体量异常庞大。**据Cybersecurity Ventures预测数据显示，2021年全球因为网络犯罪带来的损失高达6万亿美金，该数字规模已经超越了中国2020年数字经济的体量，也高于日本全国2020年的经济体量。
- **网络犯罪并没有结束，未来几年增速还将加快。**Cybersecurity Ventures预计，到2025年全球由于网络犯罪带来的损失将达到10.5万亿美元，2021-2025年平均增速约为15%。如此大规模的财富破坏和非法转移，必须予以重视并阻止。

全球网络犯罪造成的损失（亿美元）



全球网络犯罪损失与主要国家GDP对比（万亿美元）



注：日本2020年GDP为其官方公布数据进行汇率转换得到。

数据来源：世界银行、信通院、Cybersecurity Ventures、平安证券研究所

外部攻击|勒索病毒已成“全球公敌”，攻击更频繁、破坏力更强

- **勒索病毒持续活跃，攻击带来的损失持续快速扩大。**据cybersecurity ventures测算，2021年勒索软件带来的损失将达到200亿美元，预计到2031年该数字将上升到2650亿美元。从趋势上看，攻击频率正在快速上升，从2015年的2分钟一次缩短到了2021年11秒。
- **关键基础设施受到了勒索病毒的特别关照。**近年来，勒索病毒逐渐从“广撒网”转向定向攻击，表现出更强的针对性，攻击目标主要是大型高价值机构，如政府、医院、企业用户等。美国最大成品油运输管道运营商Colonial Pipeline受到黑客勒索病毒的攻击，最终支付赎金后，数据才得到解密。
- **勒索病毒的技术手段不断升级，专业化、团伙化趋势明显。**勒索病毒攻击已经从个人行为演变至团队产业，从病毒制作，到入侵攻击，再到解密沟通，都有不同的人负责运营，即分布式团伙作案，每个人各司其职，按劳分配，多劳多得。

美国最大输油管道公司遭受勒索攻击

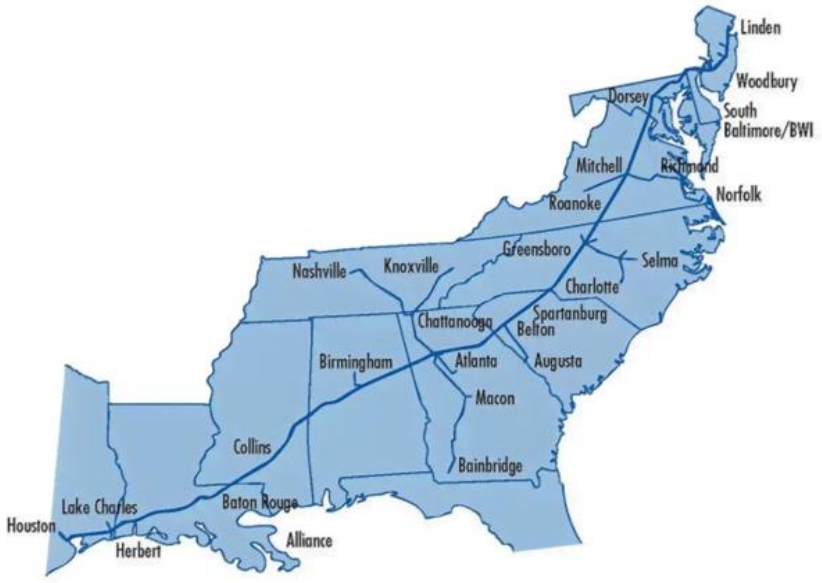
5月7日，Colonial遭受勒索病毒攻击，被迫关闭四个主要输油管线

↓

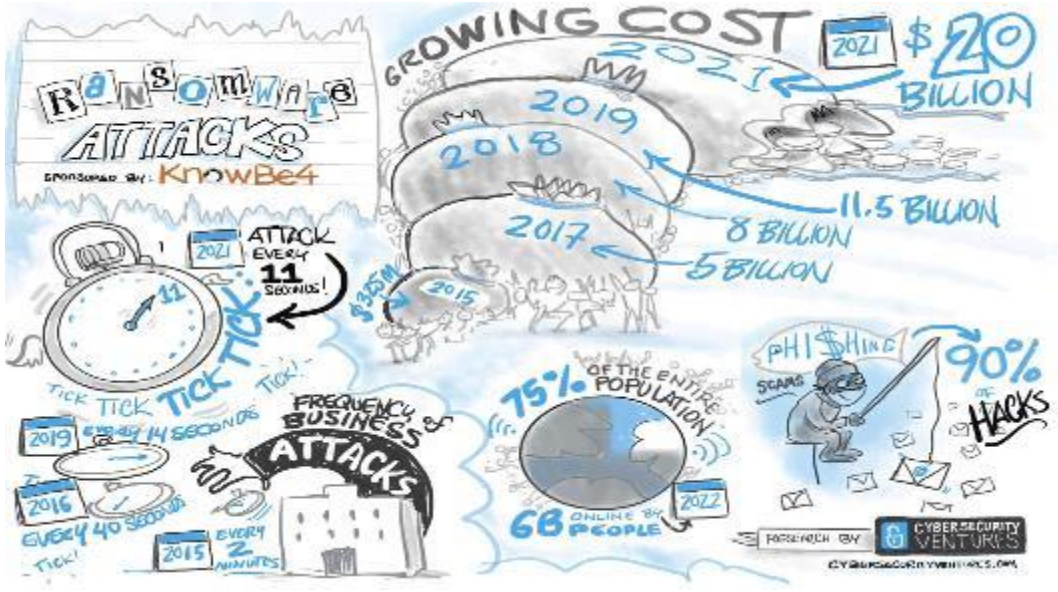
5月9日，美国宣布进入国家紧急状态，紧急启动机动车辆运输燃油，以解决美国18个州燃油需求

↓

5月13日，受黑客攻击而被迫关闭的燃油运输管道当天全线恢复运营



近年来全球勒索病毒攻击影响及频次

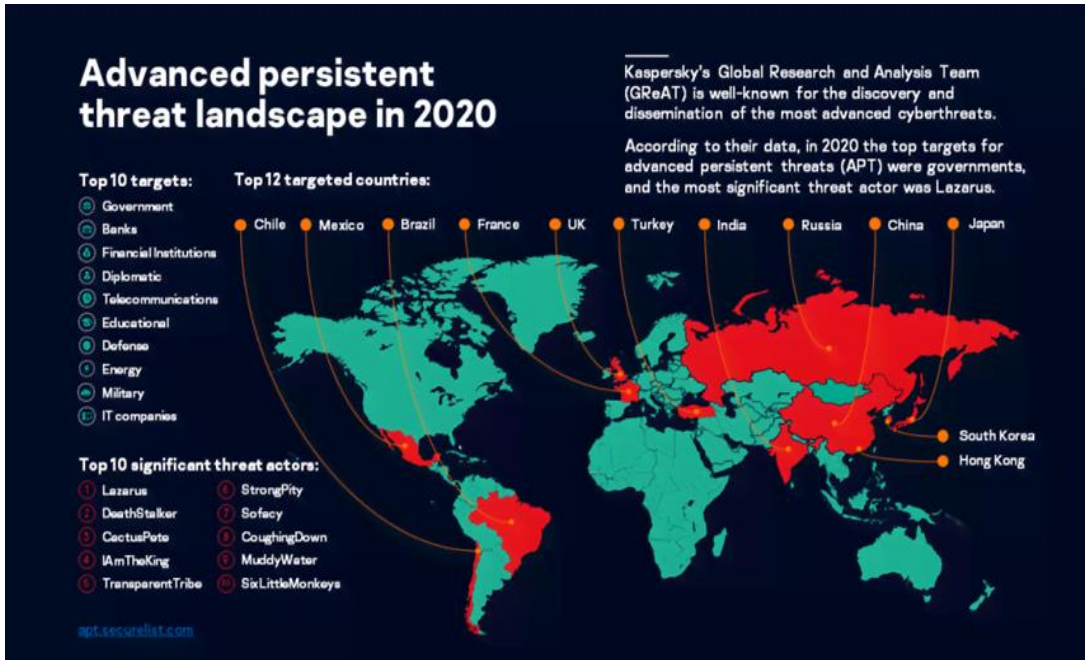


数据来源：Cybersecurity Ventures、平安证券研究所

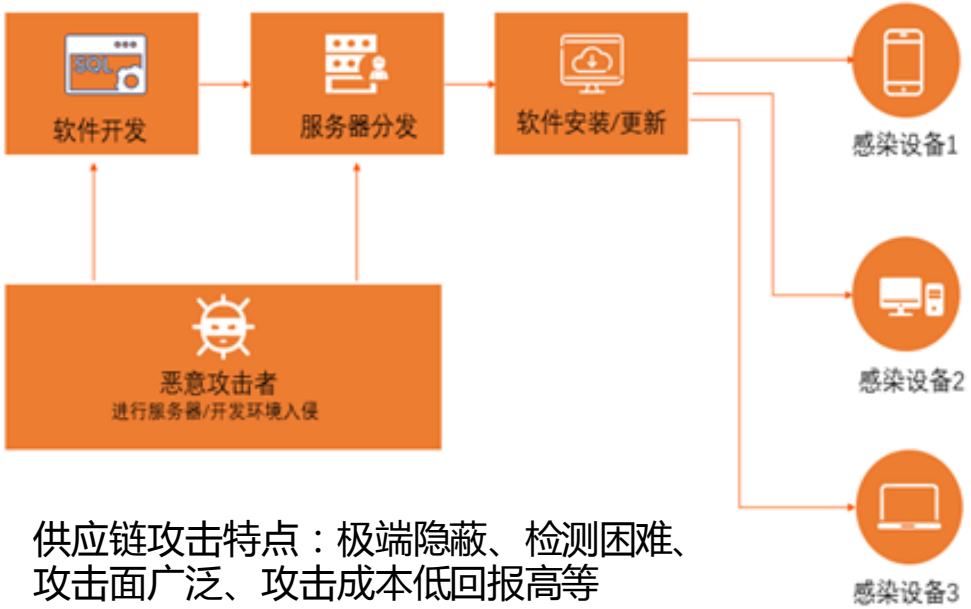
外部攻击|APT组织利用舆情、供应链攻击等模式对我进行攻击

- **APT组织盯上国内重点行业，风险上升。**APT（高等级持续性威胁）主要指某组织对特定对象展开的持续有效的攻击活动。2020年以来，主要APT组织对我国采取了不同手法的攻击：1）利用“新冠肺炎”、“基金项目申请”等社会热点以及工作邮件等为诱饵，向重点单位邮箱投放链接，引诱点击并获取账号和密码；2）利用供应链对IT业主进行攻击，典型的案例包括2020年年底爆出的“Solarwinds”攻击事件；3）利用网络攻击工具，长期潜伏在国内机构中，伺机窃取或破坏数据。
- **国内IT供应链自主性较弱，未来供应链安全为代表的APT攻击对我国IT系统、关键基础设施的影响会加剧。**

2020年全球APT攻击的目标国分布情况



APT典型攻击方式：供应链攻击



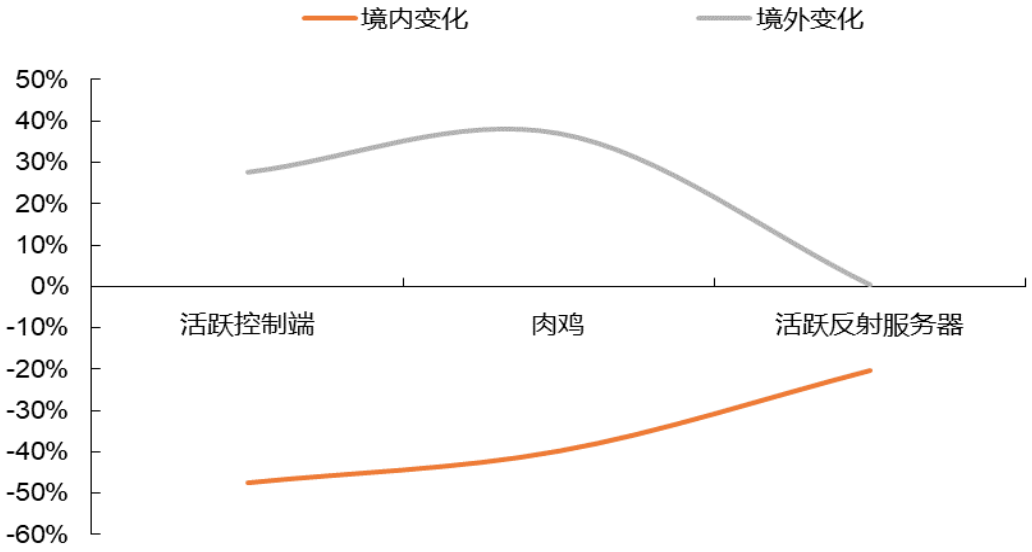
供应链攻击特点：极端隐蔽、检测困难、攻击面广泛、攻击成本低回报高等

数据来源：卡巴斯基实验室、深信服官网、平安证券研究所

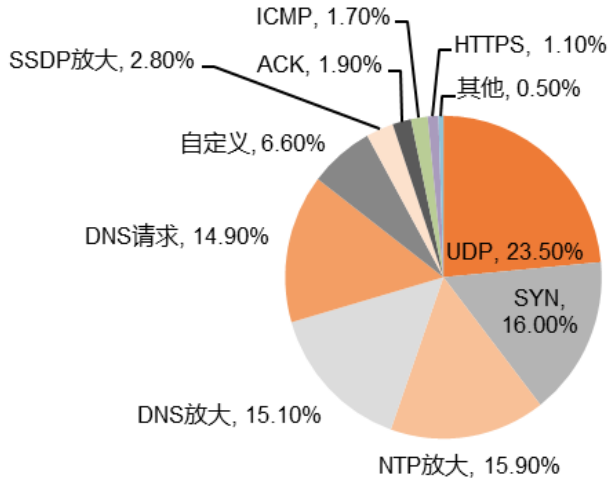
外部攻击|DDoS高带宽攻击虽被遏制，但“牛皮癣”仍难根治

- **国内“净网行动”效果开始显现，高强度攻击事件明显减少。**DDoS攻击依然是最难防范和治理的攻击方式，是网络安全行业的“牛皮癣”。2020年4月，国内开始对境内的网络进行治理，攻击资源减少明显，因此没有出现超高带宽型DDoS攻击，受到的攻击主要集中在500G-800G带宽水平。但是我们看到，攻击开始从国内转向境外，境外活跃控制端、肉鸡增长迅速。
- **攻击者为了持续获得显著的攻击效果，利用新技术使攻击手法更复杂和多样，提升攻击强度和复杂度，使得现有的防御技术更加难以缓解DDoS攻击。**2021年2季度，卡巴斯基数据显示，我国依然是全球最主要的DDoS攻击目标，移动设备和IoT正在陷入风险之中，HTTP2.0技术发展带来新的攻击手段的诞生，多种攻击手段组合攻击增多，防护难度加大。

2020年境内外攻击资源变化情况



2020年我国DDoS网络攻击类型结构

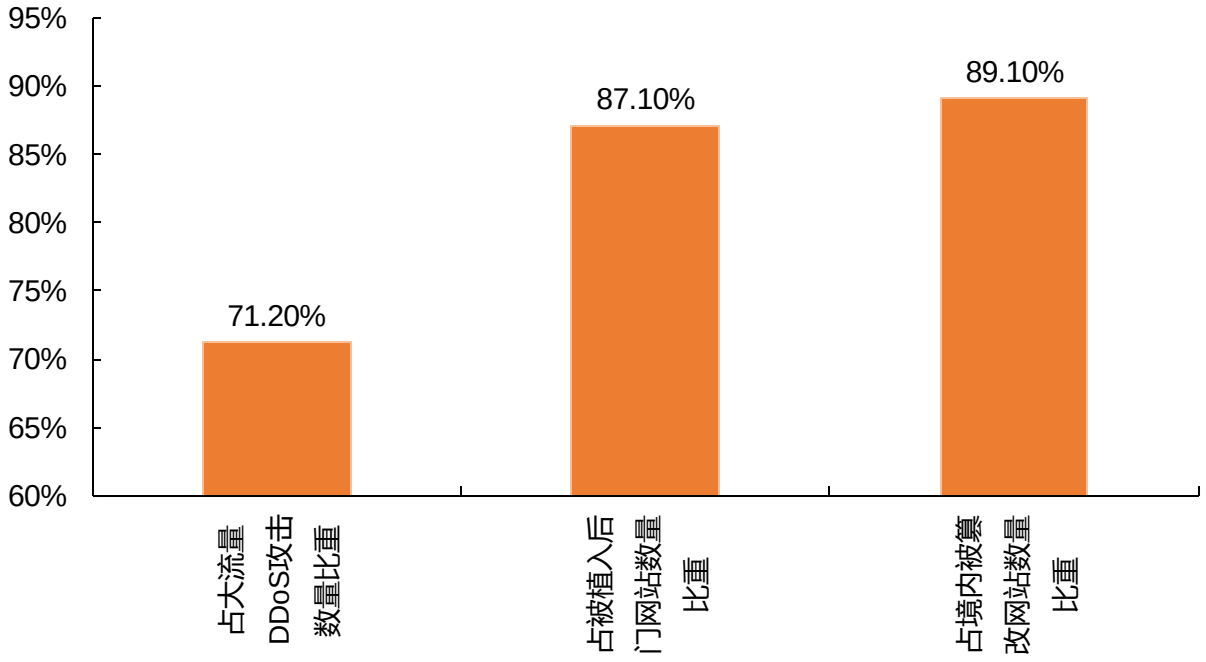


数据来源：绿盟科技、中国电信、CNCERT、平安证券研究所

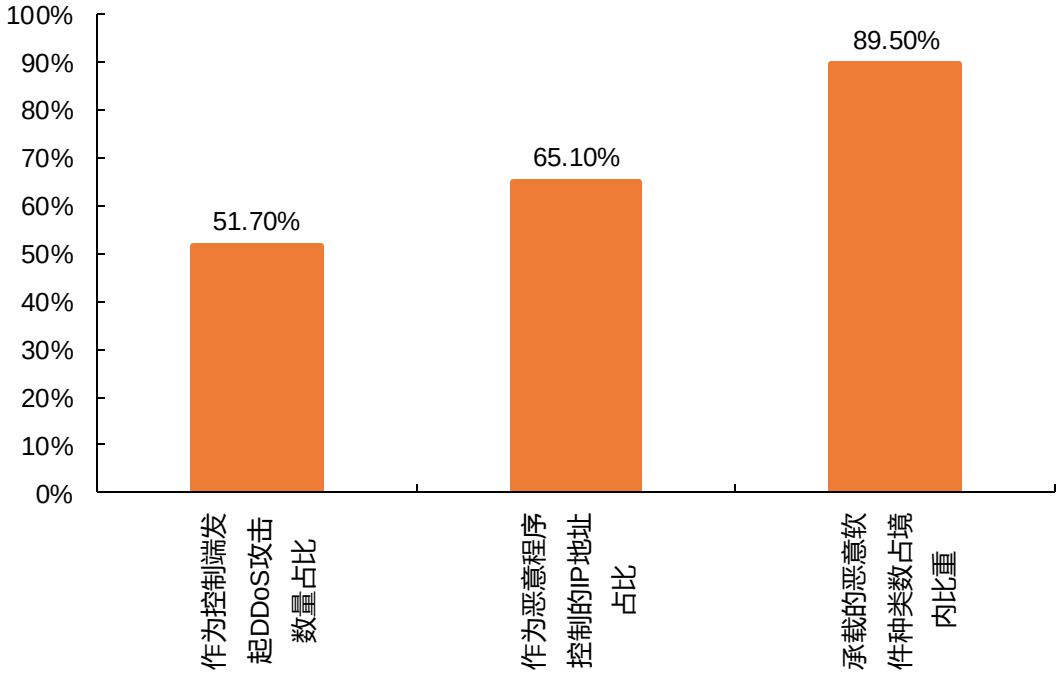
外部攻击|上云加速，但面临的威胁和风险上升

- 随着政企业务和个人应用上云的加速，云计算平台的脆弱性开始显现，针对国内云平台的攻击增多，而且利用我国云平台发起的攻击量也非常大。据CNCERT数据显示，2021年上半年国内云平台上遭受大流量DDoS攻击的事件数量占境内目标遭受大流量DDoS攻击事件数的71.2%；国内云平台被作为控制端发起DDoS攻击的事件数量占境内控制端发起DDoS攻击的事件数量的51.7%。

2021H1我国云平台受到的攻击情况



2021H1利用我国云平台发起的攻击量占比

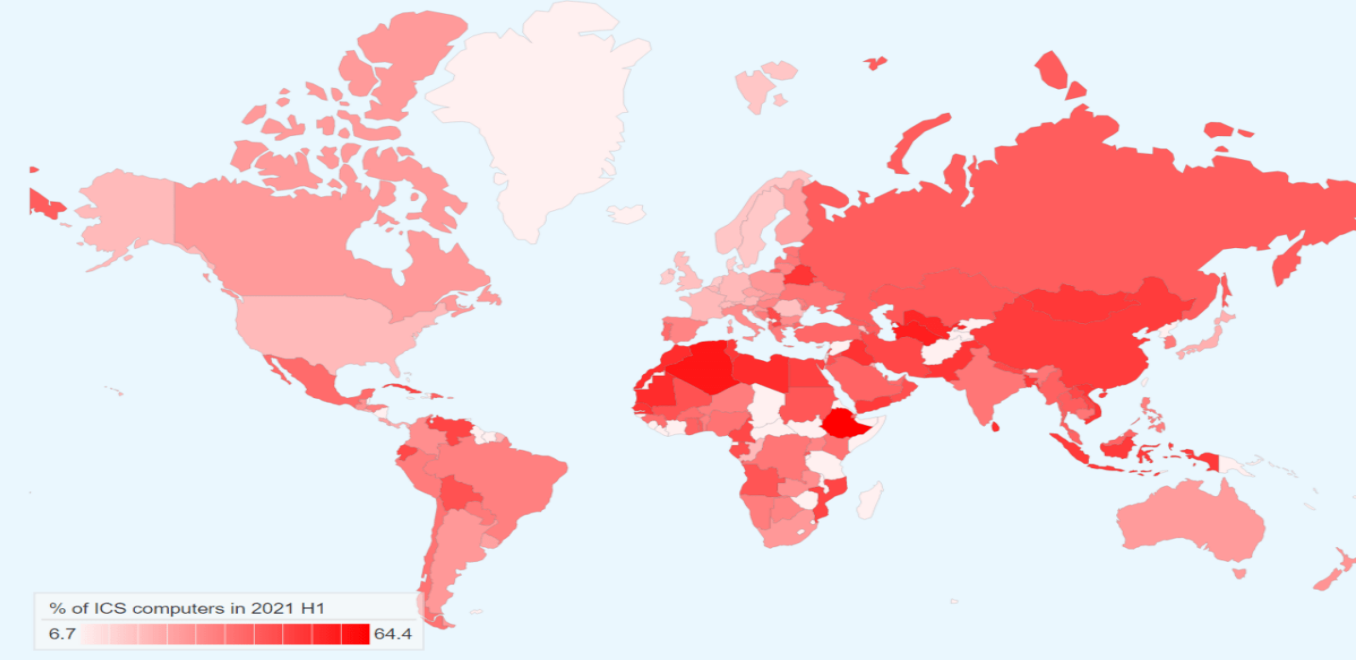


数据来源：CNCERT、平安证券研究所

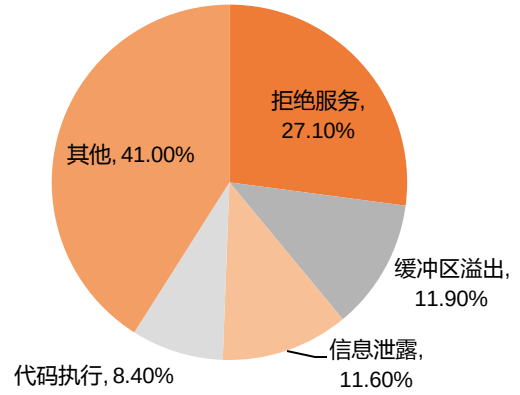
外部攻击|工控新场景扩大了防御正面，脆弱性增加

- 传统的安全防护主要关注的是用户网络和IT系统的安全，但是随着“云物移大智”技术和应用的发展，安全防护的边界明显拓宽且模糊化。新的安全领域在安全上存在很多“弱点”，非常容易成为黑客组织重点关照的对象。
- 工业企业最担心的后果是造成生产设备损坏、业务停滞，而拒绝服务漏洞排名一直靠前，如果被黑客利用，易给企业造成较大影响。从遭受攻击的行业来看，主要还是智能制造业，占比超过50%，其余行业如能源、交通、水利遭受的攻击也比较严重。

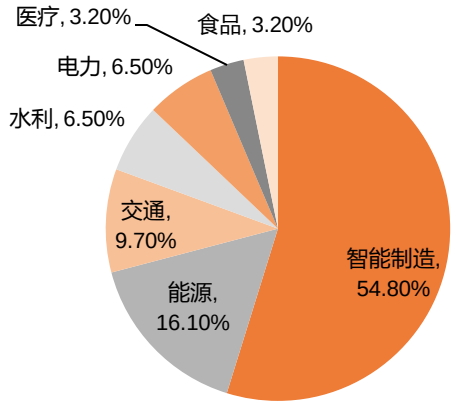
主要国家工控计算机受感染情况



国内工业控制系统漏洞类型结构



国内工业控制系统漏洞行业分布

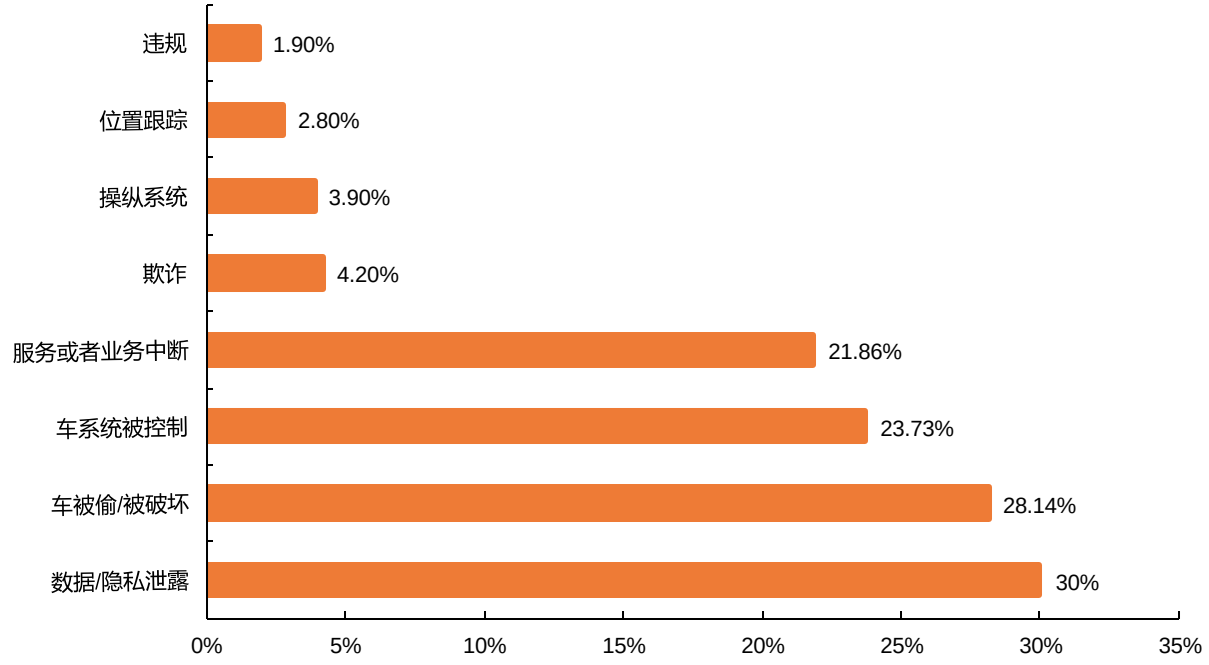


数据来源：卡巴斯基工控安全实验室、平安证券研究所

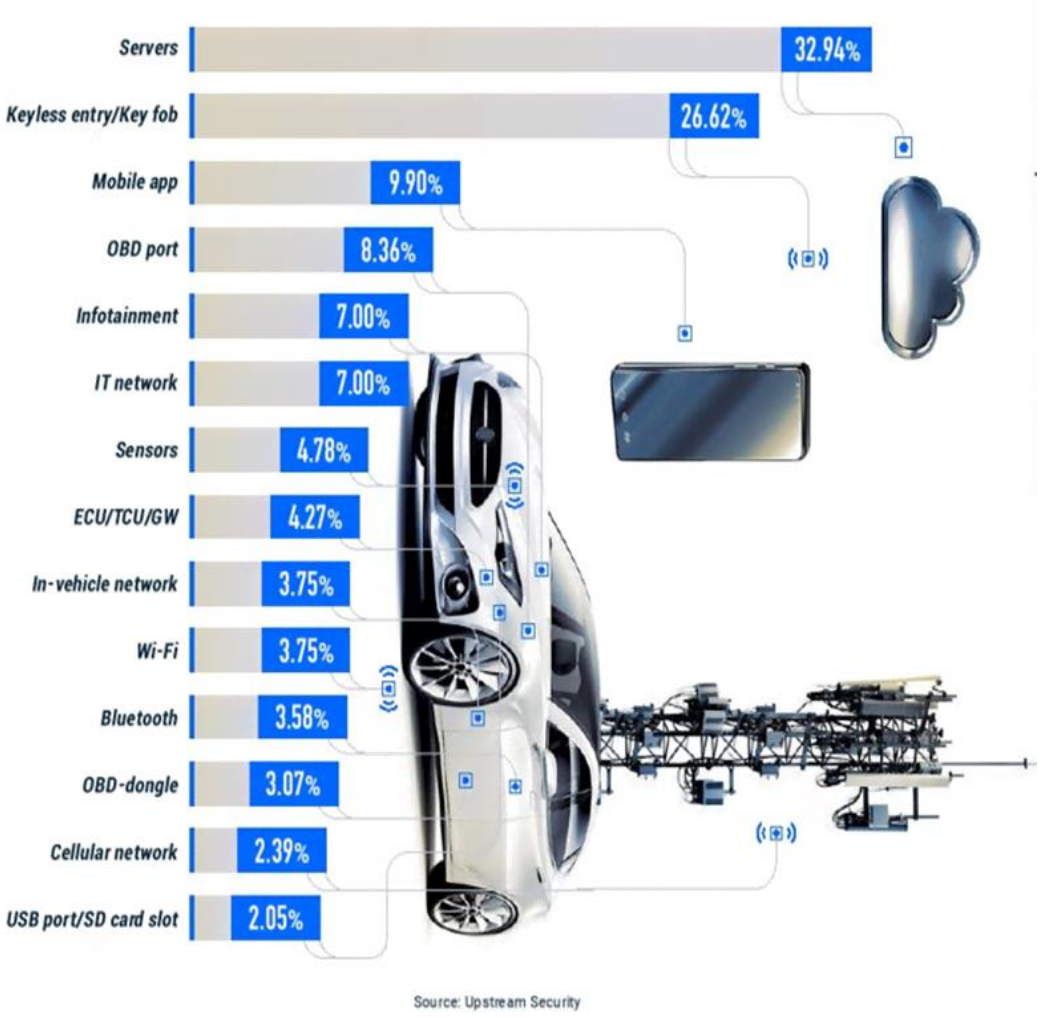
外部攻击|针对智能网联汽车的攻击大幅增加

- **随着汽车向智能化、网联化和电动化迈进，车载电子器件和软件占比大幅提升，但网络攻击也随之而来。**汽车行业庞杂的产业链、较多的攻击向量，以及海量代码带来的漏洞增加，都给智能汽车带来了巨大的风险。Upstream security数据显示，2010-2020年间，30%的攻击引起了数据或者隐私泄露，28%左右的攻击导致了汽车被偷或者破坏，另外还有24%左右的攻击导致了车辆被控制。

2010-2020年智能网联汽车攻击带来的后果



智能网联汽车攻击向量分布

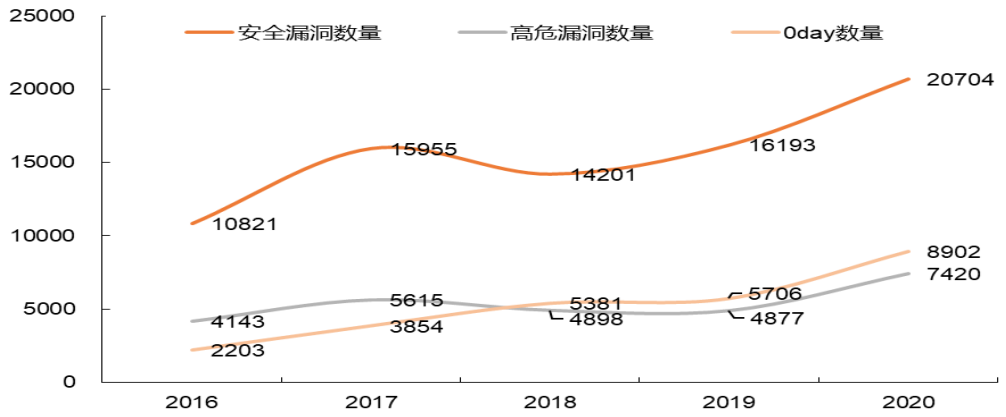


数据来源：Upstream security、平安证券研究所

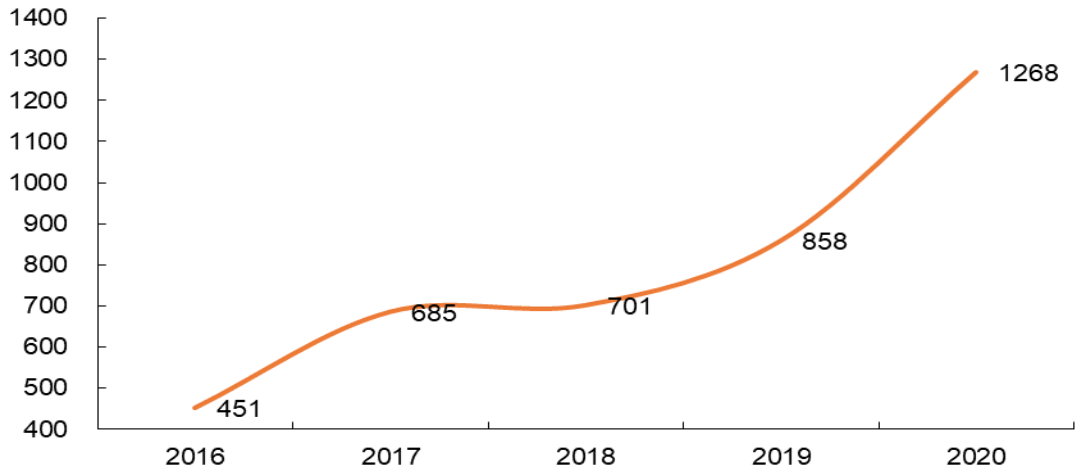
外部攻击|漏洞是攻击风险之源，数量激增且风险增加

- **攻击者主要通过漏洞对IT系统或者OT系统进行攻击。**近年来，整体漏洞数量、高危漏洞和0day漏洞数量呈现出快速增长态势，尤其是一些经典漏洞如永恒之蓝等，还在被攻击者利用；移动互联网、电信和工业控制等重点行业漏洞数均在明显上升。
- **从长期来看，漏洞问题预计将趋于严重，短期内很难得到根治。**以全球软件巨头微软发布的漏洞为例，这些年以来发布的漏洞数是呈现出大幅上升的态势，2020年更是创出新高，完全杜绝漏洞的可能性微乎其微。

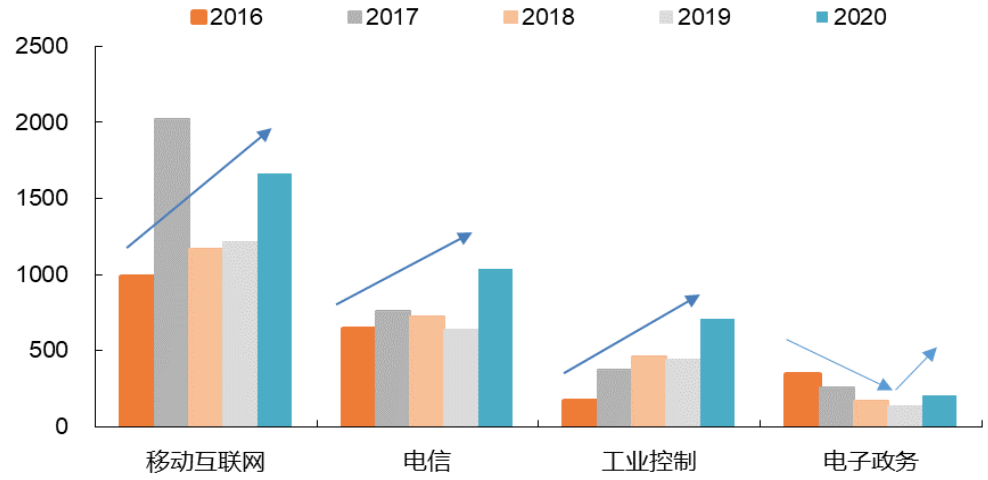
我国安全漏洞数量（个）



微软历年发布的本公司产品漏洞数（个）



2016-2020年主要行业漏洞数量变化（个）

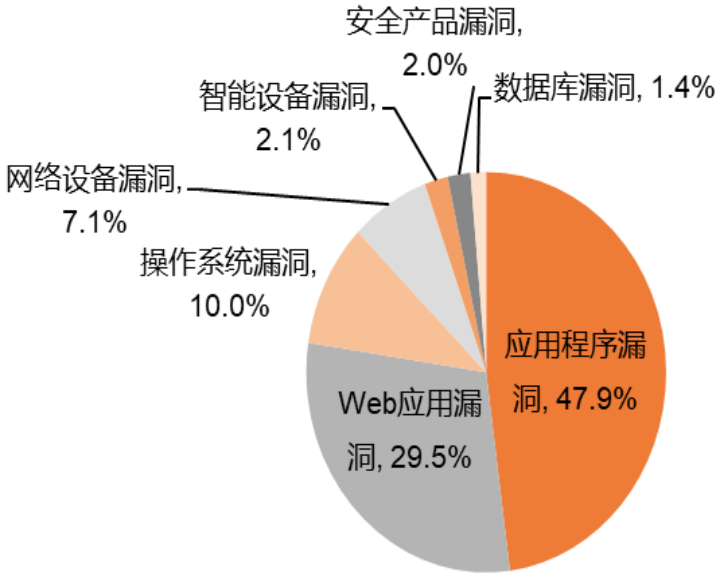


数据来源：《微软漏洞报告2021》、CNVD、平安证券研究所

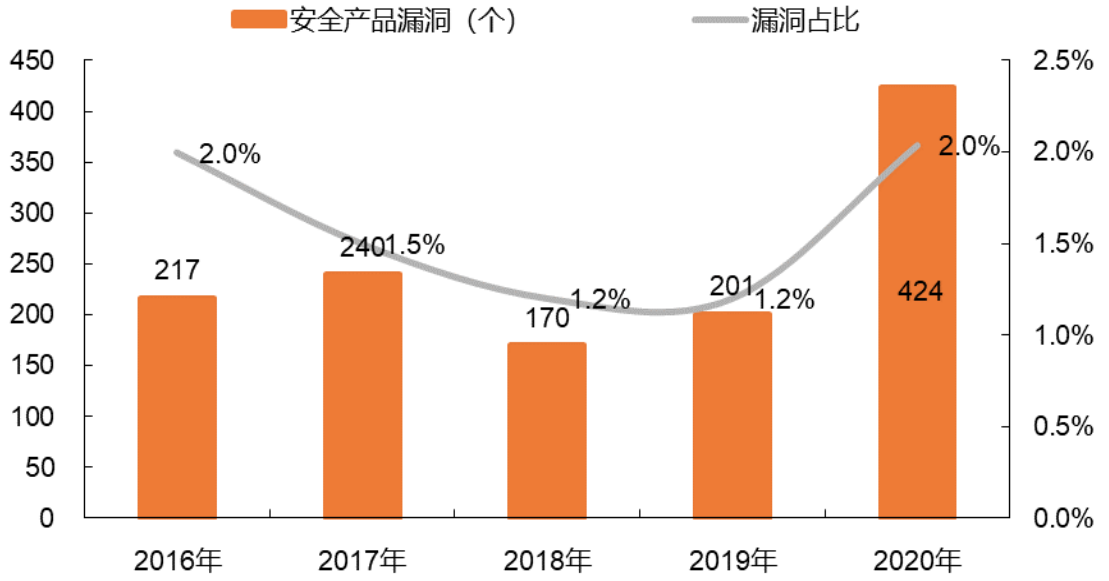
外部攻击|网安产品自身漏洞占比上升，安全威胁严重

- 由于网络安全防护产品在网络安全防护体系中发挥着重要作用，且这些产品在国内使用范围较广，相关漏洞一旦被不法分子利用，可能构成严重的网络安全威胁。CNVD收录的通用型漏洞中，网络安全产品类漏洞数量达424个，同比增长110.9%，网络安全产品自身存在的安全漏洞需获得更多关注。
- 终端安全响应（EDR） 系统、堡垒机、防火墙、入侵防御系统、威胁发现系统等网络安全防护产品多次被披露存在安全漏洞。

2020年国内通用型漏洞结构



安全产品漏洞数量及占比

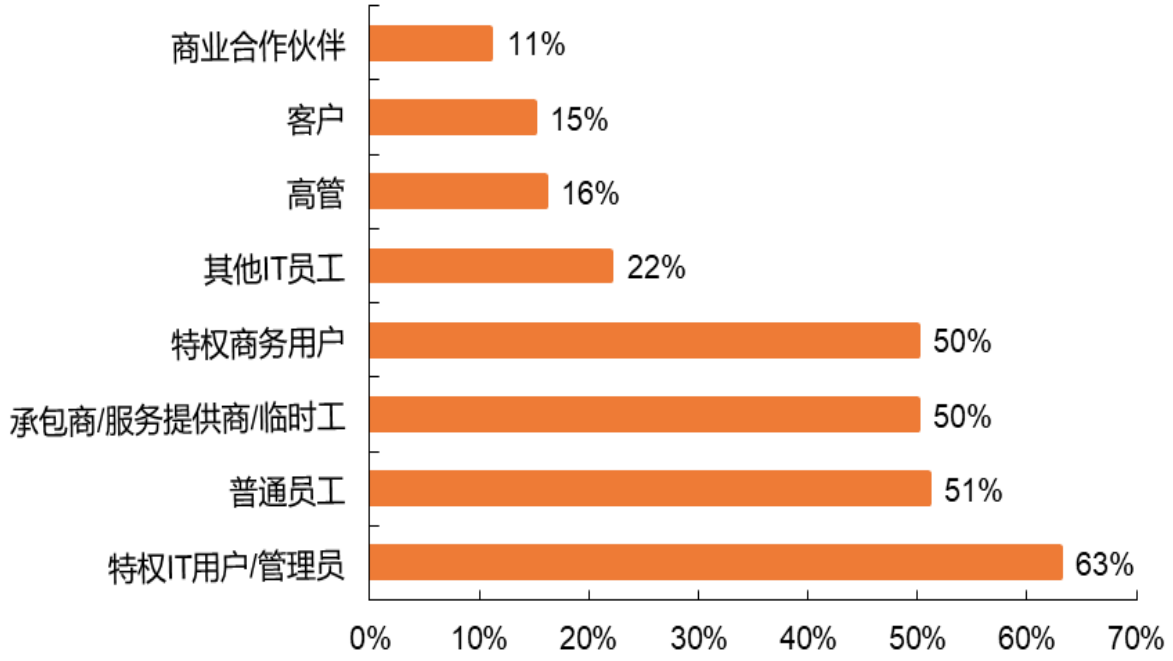


数据来源：CNVD、平安证券研究所

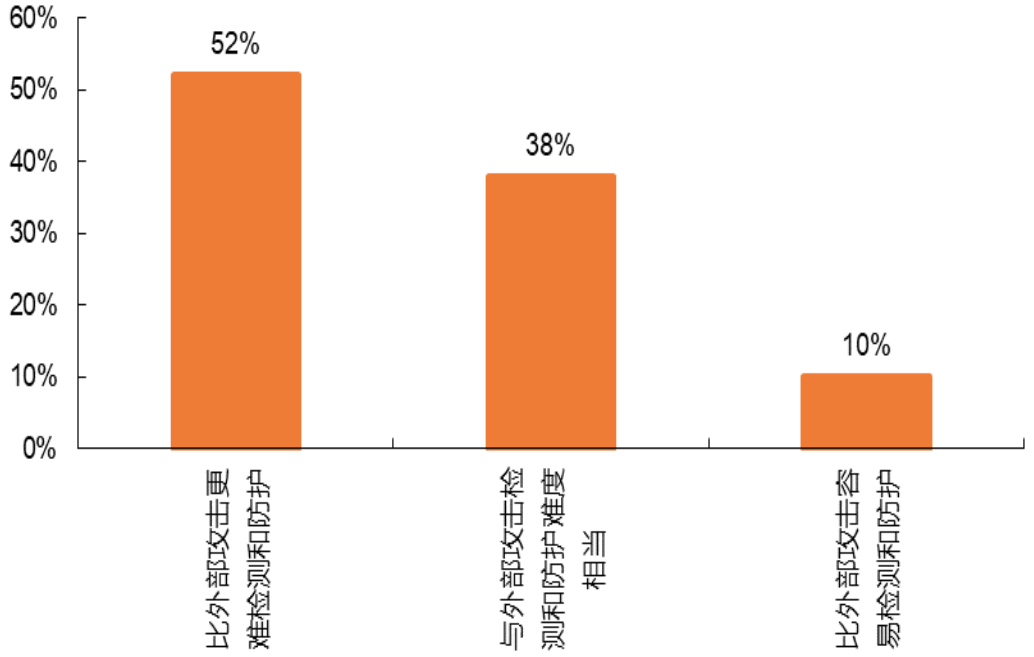
内部风险|内部人员对机构的安全影响上升，权限管理难度大

- Cybersecurity Insiders公布的调研数据显示，2019年，68%的调研对象认为所在公司遭受了内部攻击，70%的受访者公司至少遭受了一次内部网络攻击。其中，特权IT用户和管理员、普通员工、承包商、特权管理人员可能都会引发内部攻击风险。
- 相较于外部攻击，内部攻击难以发现和检测到。调研数据显示，52%的受访者认为内部攻击的检测比外部攻击更难，尤其是企业上云之后这项工作难度将更大。

内部攻击主要来源和占比



内部攻击与外部攻击防护难度对比



数据来源：Cybersecurity Insiders、平安证券研究所

合规侧 | 法律框架搭建完毕，数据安全重要性提升明显

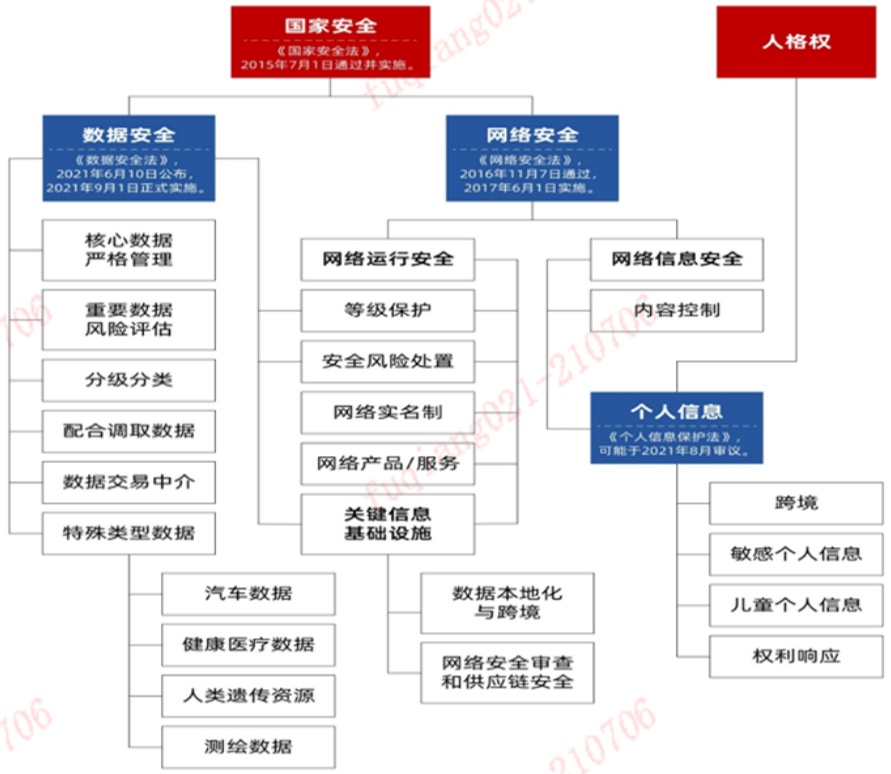
数据安全成为监管主题。此前合规关注的重点在系统的安全性，最终的结果就是“围墙式防护”，运营者投入多是在边界上。但是，随着国家之间对数字主权竞争的持续加深，欧盟、美国和日本都在通过立法加强数据保护，我国必然也要加强，否则就会成为数字监管低谷，不利于国内数字要素的应用。2021年6月，人大通过《数据安全法》。此后，在美上市的滴滴出行等公司，受到网络安全审查。尤其是在7月10日，网信办还修订了《网络安全审查办法》，将《数据安全法》作为依据，对境外上市企业进行审查。

“三足鼎立”的法律体系搭建完毕。从整体看，中国网络数据领域的法律体系是以三部法律为基础的，分别是《网络安全法》、《数据安全法》和《个人信息保护法》，我们形象地称它为“三足鼎立”，其中《网络安全法》已经公布实施；《数据安全法》已经公布，今年9月1日正式实施；《个人信息保护法》8月20日人大通过，11月1日正式实施。此外，市场上持续关注的《关键信息基础设施安全保护条例》也在7月30日正式公布。

2019年以来国内网络安全行业政策情况

发文机构	文件名称	发文时间
工信部	《关于加强工业互联网安全工作的指导意见(征求意见稿)》	2019.4
国家标准委	《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 网络安全等级保护测评要求》、《信息安全技术 网络安全等级保护安全设计技术要求》（等保2.0标准）	2019.5
中央网信办	《数据安全管理办法（征求意见稿）》	2019.5
工信部	《国家网络安全产业发展规划》	2019.6
工信部	《网络安全漏洞管理规定（征求意见稿）》	2019.6
人大	《密码法》	2020.01
国家网信办等部委	《网络安全审查办法》	2020.04
人大常委会	《数据安全法》（已通过）	2021.06
国家网信办	《网络安全审查办法（修订意见稿）》	2021.07
国务院	《关键信息基础设施安全保护条例》	2021.07
工信部等	《网络产品安全漏洞管理规定》	2021.07
人大	《个人信息保护法》（通过）	2021.08
工信部	《关于加强车联网网络安全和数据安全工作的通知》	2021.09

国内网络安全法律体系构成



数据来源：政府网站、观察者网、平安证券研究所

合规侧 | 数据安全管理制度机制将建立，分级分类是重点

中国平安 PINGAN
金融 · 科技

数据分类分级保护，重要数据保护	数据安全审查	数据安全风险监测预警	数据安全应急处置
数据出口管制	数据交易管理	数据安全检测评估、认证	数据安全标准
数据安全教育培训	歧视性对等措施	政务数据开放	……

合规|重要数据识别标准已明确，数据安全监管基础性问题解决

- 《数据安全法》要求对数据实行分类分级保护，并加强对重点数据的保护。由于对“重要数据”的监管，多部法律都对该内容有监管要求，因此重点数据的范围和确认标准，对机构或者企业是否纳入监管十分重要，也解决了行业监管的基础性问题。2021年9月底，国家市场监督总局、国标委对外发布了《重要数据识别指南》（征求意见稿），明确了“重要数据”的划分范围和流程。按照该意见稿，监管将从8个特征去判断数据是否为重要数据。

目前国家对重要数据的监管要求

类别	具体内容
第一类	《网络安全法》第37条和《数据安全法》第31条对重要数据出境提出的安全管理要求。
第二类	《数据安全法》第21条提出的制定重要数据目录要求。
第三类	《数据安全法》第27条提出的明确数据安全负责人和管理机构、第30条提出的定期开展风险评估等责任义务要求。
第四类	《网络安全审查办法》修订时，要求将核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险，作为采购活动、数据处理活动以及国外上市可能带来的国家安全风险因素。
第五类	国务院办公厅2021年立法计划中，已经要求网信办牵头制定的《数据安全管理条例》。该条例料将对重要数据安全保护提出一整套监管制度。
第六类	根据《数据安全法》第27条要求，在等级保护基础上履行数据安全保护义务，据此下一步的等级保护工作中有可能会强调对重要数据保护的要求。
第七类	目前全国信安标准正在组织制定的其他数据安全标准中（例如《网络数据处理安全规范》），已经全面引入了“重要数据”概念。这些标准将逐步落实法律法规要求、细化对重要数据的保护规定。

重要数据的特征和内涵

特点	分类	具体内涵	特点	分类	具体内涵
与经济运行相关	反映战略储备情况	粮食、物资、能源等储备数据	与科学技术相关	涉及出口管制物项、特殊知识产权、重大发明发现、国家科技计划	-
	支撑工业生产	工业控制数据、研发数据、重要装备数据	与安全保护相关	物理安全	重要场所与目标、安保装备、安保部署、危化品等数据
	支撑重点行业	关键信息基础设施运营的核心业务、经济运行、供应链数据		网络安全	关基网络防护信息、规划建设、运维数据、漏洞与重大事件、应急通信、无线电数据等
	与统计相关	公布前的数据；统计调查中的原始数据	与应用服务相关	用户委托数据	向用户提供服务转移过来的数据等
与人口与健康相关	反映人口情况	非公开人口普查数据等		用户使用数据	公共基础设施产生的用户信息
	涉及医疗健康	诊疗与健康管理信息	与政务相关	国家机关产生的数据	不宜公开的文件和资料等
		疫情管理信息		公民上报数据	
	涉及医药食品情况	药品实验数据等	其他	-	-
与自然资源与环境相关	地理信息	地图、导航、特殊测绘、重点目标地理信息等			
	涉及水利、气象、环保检测等情况	-			

资料来源：《重要数据识别指南》（征求意见稿）、网安网、平安证券研究所

小结|安全环境变迁明显，供给侧需要因势而动

中国平安 PINGAN
金融·科技

攻击侧

- 网络攻击组织化、隐蔽化、黑产化
- APT攻击增多，勒索病毒泛滥，DDoS攻击出现新特点
- 新技术被滥用，云、大数据和人工智能等技术被用来作恶
- 内部攻击问题凸显

需求侧

- 理念变化，由外向内
- 数字化转型加速，新场景如云、数、工、移等新场景安全需求增加
- 数据资产增多，单点防护变为全系统防护，注重防护实效
- 合规需求增多
- 安全服务需求上升

网络安全

监管侧

- 《数据安全法》出台，监管趋严、更为细化
- 《网络安全审查办法（修订意见稿）》
- 《关键基础设施保护条例》
- 《个人信息保护法》

供给侧

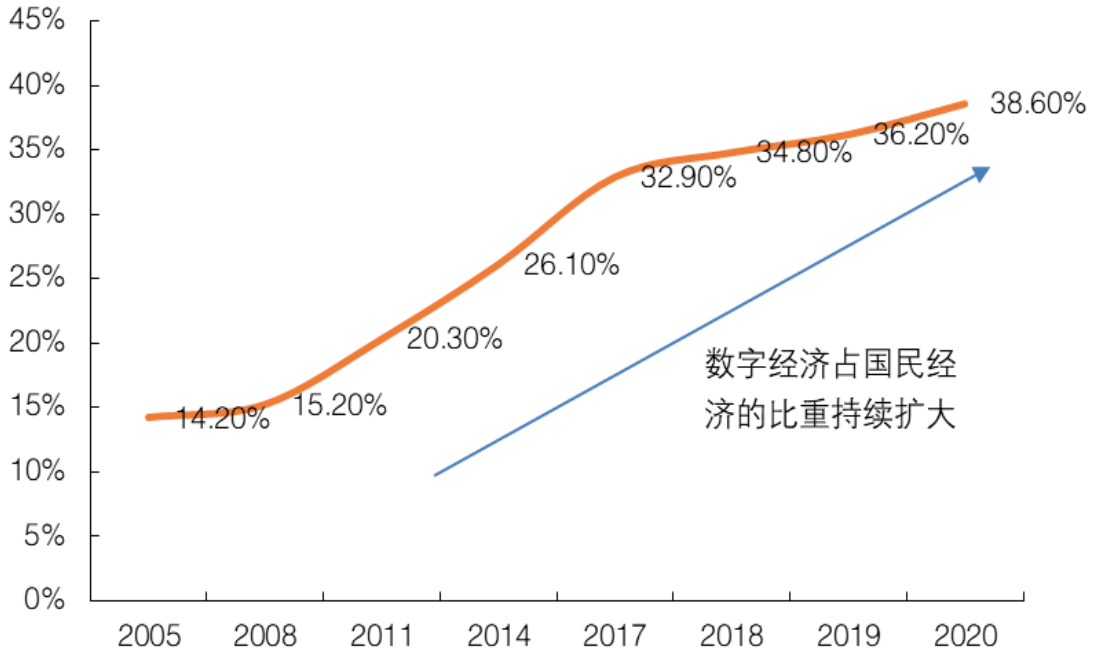
- 完善产品体系适应变化
- 新技术应用（人工智能、大数据、隐私计算等）
- 合规解决方案趋于完善
- 布局云计算、数据审计、工控及物联等新安全场景
- 加码安全服务能力建设

目 录 CONTENTS

趋势|网安行业进入新的“拐点”期，与信息化融合提速

- 从整个网络安全发展主脉络来看，无论是“攻防”还是“合规”，最核心的逻辑还是信息化重要了，安全才更重要。信息化、数字化发展越快，对关键基础设施运营、机构和企业业务开展的影响也就越大，威胁和风险也将持续上升，网络安全增长才会提速。
- 2021年以来，国内对数字经济的发展特别关注，信息化已经渗透到国民经济的各个领域，产业数字化、数字产业化、数字化治理产业规模快速扩大，新的威胁和挑战在增加，安全同信息化、同业务在深度融合。

数字经济占国民经济的比重



我国网络安全发展经历的阶段划分

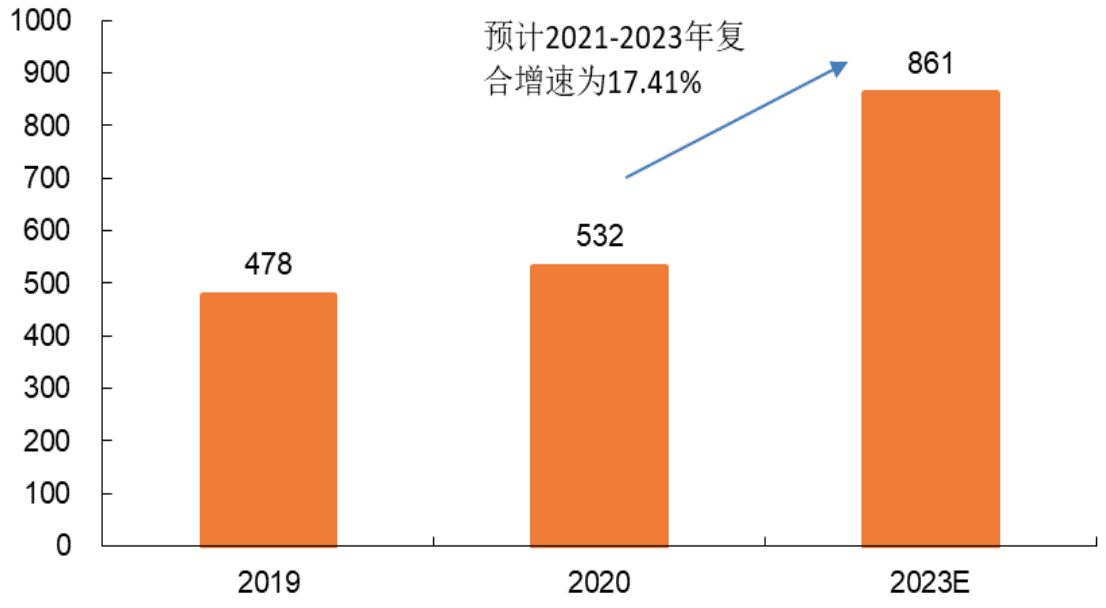
	1995-2004	2005-2014	2015-2020	2021-未来
特点	信息化对于业务是辅助性的，网络安全也处于非常初级的阶段。	信息化开始跟业务结合，网络安全也随着合规趋严和威胁升级变得越来越重要。	随着全面数字化转型，信息化与业务深度融合，信息系统的安全与业务稳定运行高度相关。	数字化已经开始贯穿于经济社会发展的全领域、各层级，成为国家治理、经济发展和社会运行的核心驱动力。
行业发展	网安行业发展很慢，规模很小，每年只有几十亿规模，十年间复合增长率只有5.8%。	在等保合规和应对威胁驱动下，网络安全产业开始加速，年产业规模开始超过250亿，10年间复合增长率也超过了10%。	网络攻击更为复杂化、组织化和黑产化，关键基础设施和数据受到的威胁增加，网络安全行业发展较快。	法律法规、政策制度和监管手段密集出台，安全应对新技术也在出现，网络安全占信息化比重将提升。
与信息化投入的关系	重视程度不高	先发展后治理	同步发展同步治理	前瞻性部署，融合发展

资料来源：信通院、安全内参、平安证券研究所

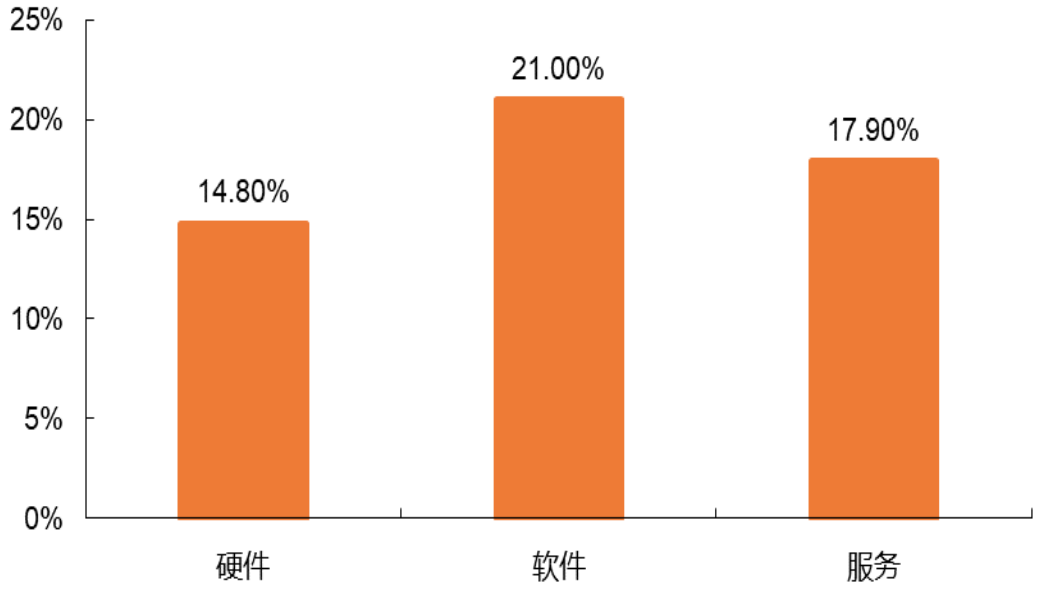
趋势|新时期，国内网络安全行业将保持中高速增长

- “十四五”时期，国内数字经济将保持快速发展势头，围绕着数据资产的攻防需求也将更为旺盛。尤其是在合规趋严的大背景下，重点行业如电信、金融、能源等行业网络安全投资占比将大幅提升至10%左右，同时中小企业和一些关键场景的安全投入力度也将加大。我们基于CCIA口径，预测到2023年行业市场规模有望达到861亿元，预计2021-2023年平均增速约将达到17.41%。其中软件业务平均增速将超过20%。
- 分具体领域看：硬件投入主要集中在统一威胁管理类产品、安全内容管理、入侵检测与防御“三大件”；软件主要增长点在网络安全分析、情报、响应与编排等方面；安全服务则主要是依托安全咨询（合规咨询、安全测试和应急响应等），托管运营服务可能是服务板块增长最快的子类。

国内网络安全行业收入预测（亿元）



2021-2025年国内网络安全各领域增速预测

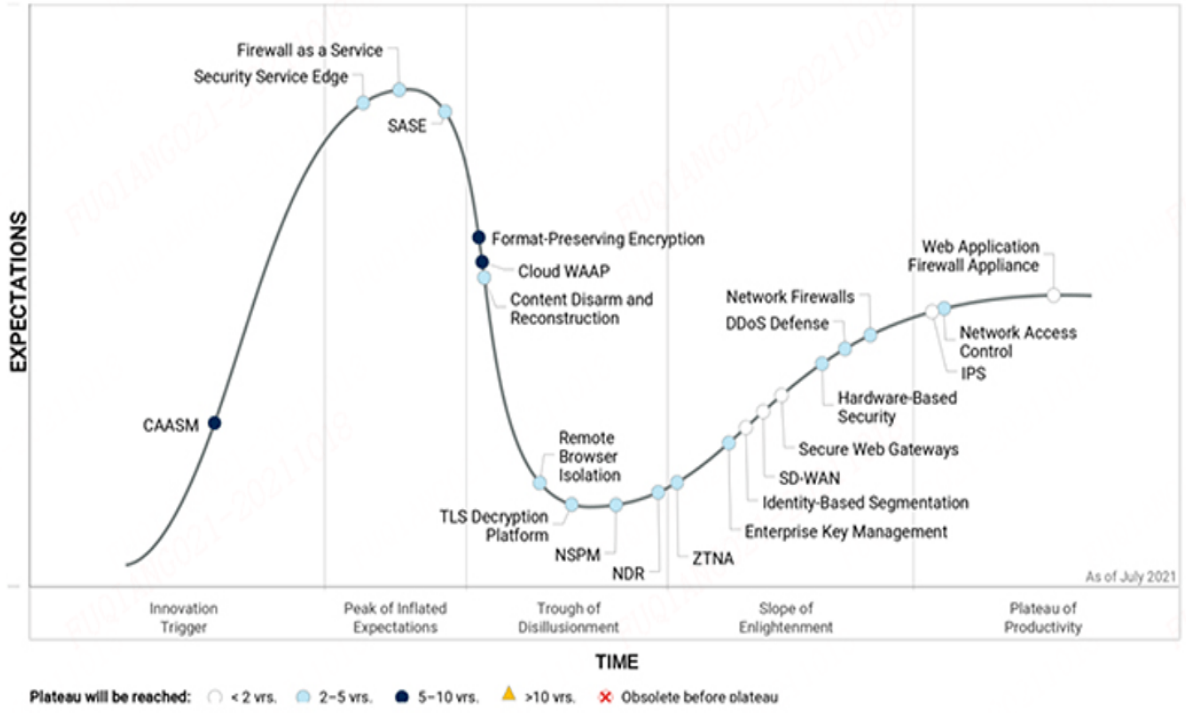


资料来源：中国网络安全产业联盟（CCIA）、平安证券研究所

趋势|技术创新活跃，云安全、安全服务化是趋势

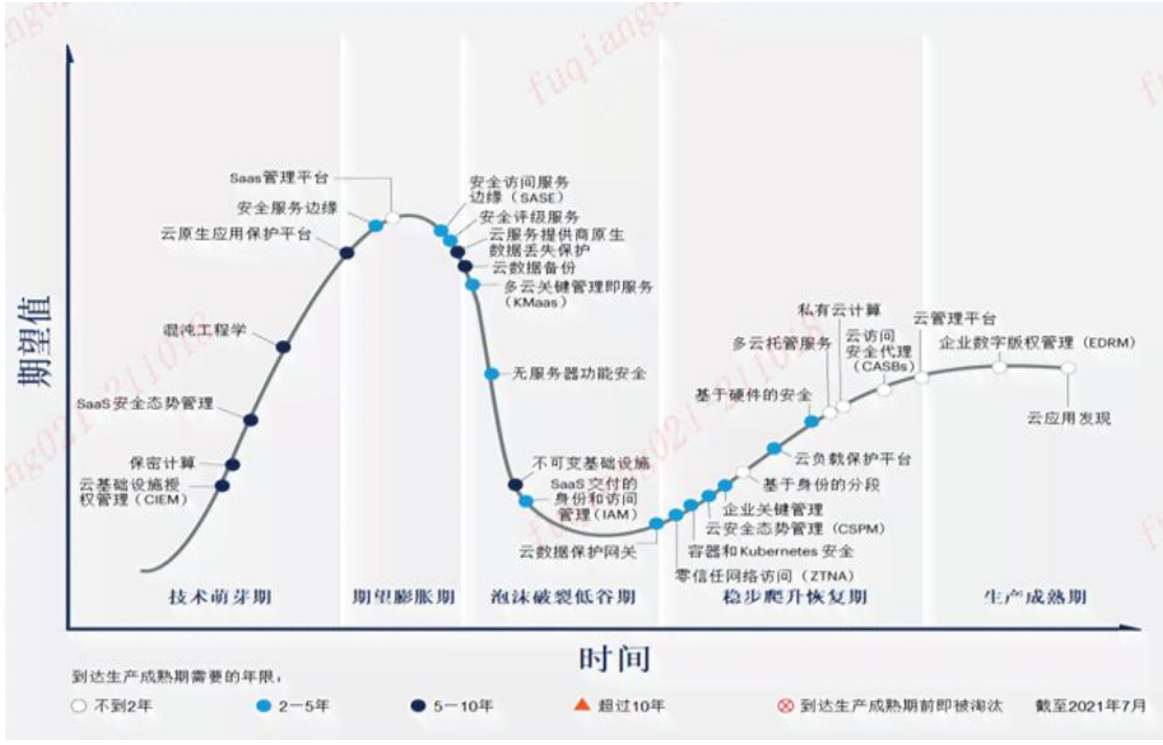
- 网络安全整体创新活跃，应用性强。从Gartner技术成熟度曲线看，多数网络安全技术都处在曲线的右侧，意味着它们正在接受市场的验证，短期内有希望走向成熟，比如零信任、硬件安全、抗D、网络接入控制等；目前处在炒作高点的SASE、防火墙即服务，也可能在2-5年内得到市场的广泛应用。
- 2021年，云上业务负载有望超越私有数据中心，移动办公、数字化业务对云上安全技术的需求增长快速。从Gartner技术成熟度曲线来看，云管平台、多云托管服务、硬件安全等市场已经相对成熟，零信任、容器安全、SASE（安全访问服务边缘）有望在未来2-5年内走向成熟。

2021年网络安全技术成熟度曲线



Source: Gartner (July 2021)

2021年云安全技术成熟度曲线

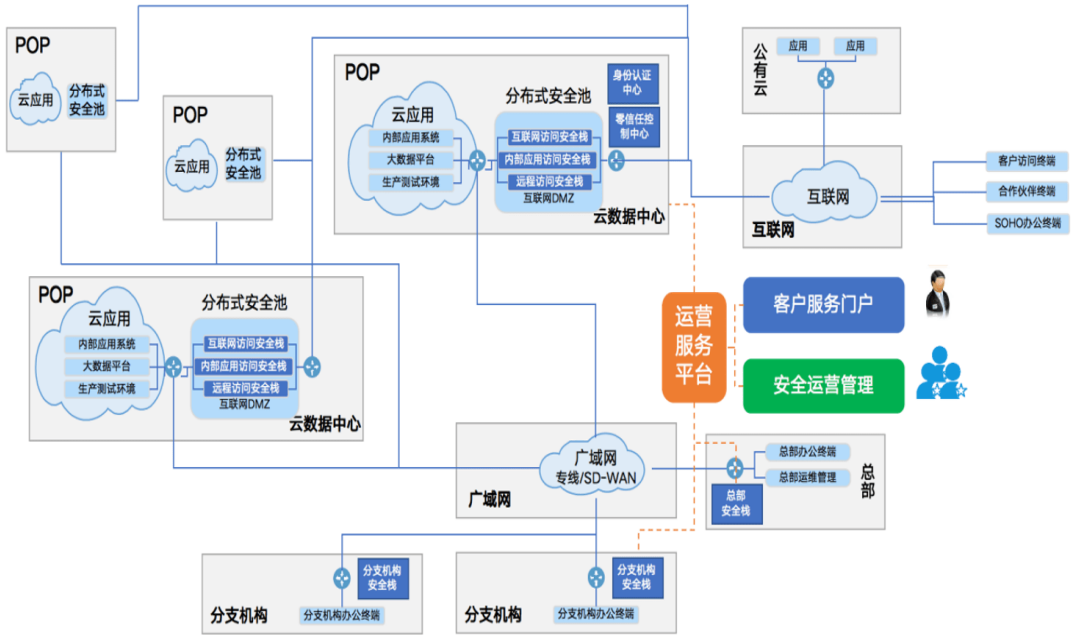


数据来源：Gartner、平安证券研究所

趋势|云安全访问服务开始落地，推动安全云化交付

- 边缘计算和云基础设施的推广，加上近期远程办公的飞速增长，给传统网络架构和安全模式带来了严峻挑战。为应对这种趋势，安全供应商、云供应商和网络供应商推出了新型软件定义和云交付解决方案，将网络即服务和网络安全即服务功能整合到了一起。
- 2019年底，Gartner 首次提出 SASE（安全访问服务边缘）的概念，定义是将基于软件定义广域网（SD-WAN）的基础设施与网络安全功能结合，以云的方式交付，在企业数字化转型的场景下，满足企业动态访问网络的安全需求。Gartner 预计，到 2024 年全球至少40%的企业已经接入 SASE 或计划采用 SASE来取代传统的硬件解决方案。

奇安信安全访问服务的体系架构



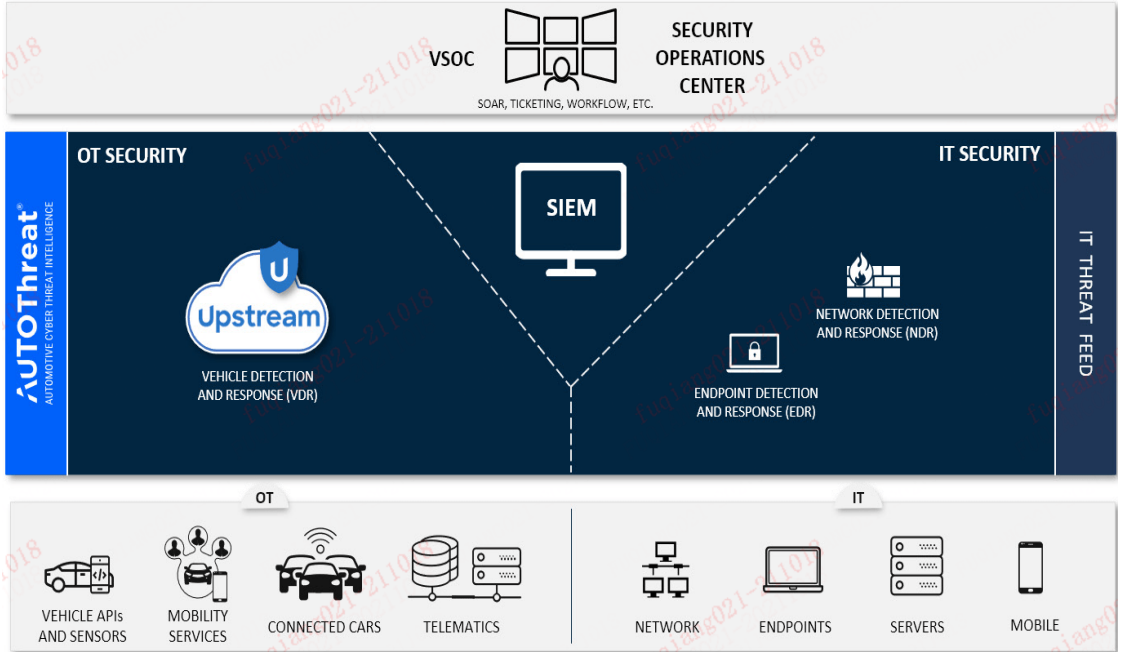
深信服云安全访问服务（Sangfor Access）架构图

数据来源：奇安信、深信服、平安证券研究所

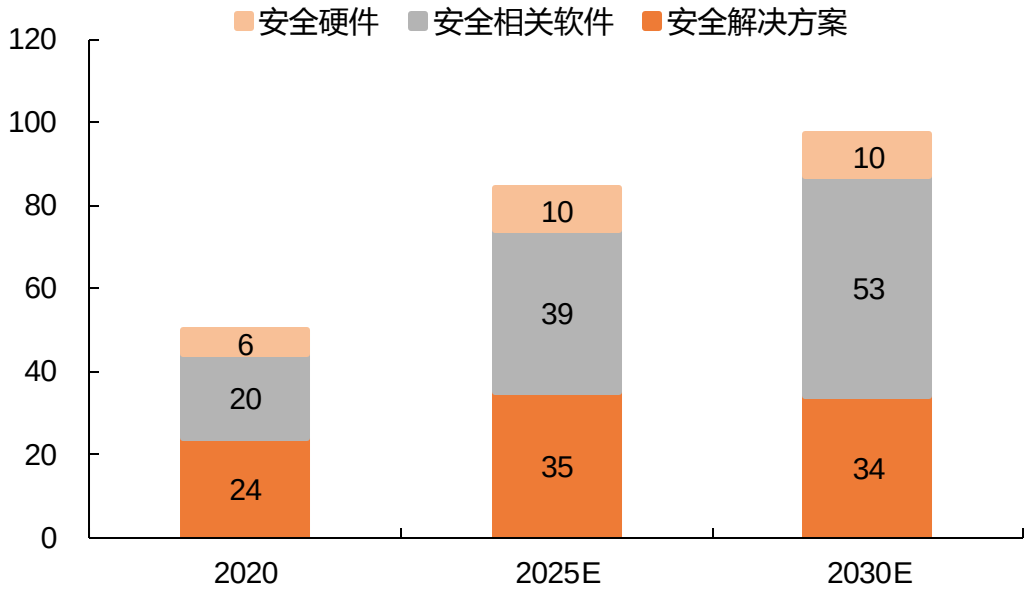
趋势|类似IT网络安全，智能汽车安全体系也将建立

- 据车联网安全公司Upstream security预测，到2023年，联网汽车预计将占全球所有乘用车的1/4。随着高等级自动驾驶的落地，到2025年，联网汽车将占全球汽车市场的近86%。从市场规模上看，据麦肯锡预测，2025年全球汽车网络安全市场规模有望达到84亿美元，其中安全软件将逐步取代解决方案成为汽车网络安全最大的市场。
- 按照Upstream security的推荐的方案，面向智能汽车安全市场，也将建立起与IT系统类似的安全运营中心（VSOC）、车端检测响应平台（VDR）、网络检测响应平台（NDR）、安全信息和事件管理平台（SIEM），实现车联网全生命周期的安全防护。

Upstream security智能汽车安全运营中心架构



2020-2030年全球汽车网络安全市场规模及结构（亿美元）



数据来源：Upstream security、麦肯锡、平安证券研究所

趋势|隐私计算全面启动，开始应用于数据交易等场景

- **整体监管趋严的大背景下，隐私计算应用增多、市场开始启动。**隐私计算可以在保护数据隐私的前提下，解决数据流通、数据应用等数据服务问题，实现不共享数据而是共享数据价值，对数据进行安全保护与脱敏。目前在金融、医疗、政务以及数据交易等领域都在应用。据毕马威等机构预测，到2024年，隐私计算相关技术服务营收有望触达100-200亿人民币的市场，甚至将撬动千亿级的数据平台运营收入空间，国内企业如安恒信息、神州数码等都推出了相关解决方案。

隐私保护技术防护体系

安恒信息隐私计算应用方案（数据安全岛）

数据来源：毕马威、安恒信息、平安证券研究所

趋势|国际同行先行一步，通过并购发力数据安全等领域

- 相较而言，国内网络安全还在起步阶段，安全投入和技术同国际先进水平还有较大差距。从新技术应用程度和发展阶段角度看，国内还处在追赶状态。从海外主流企业并购的方向看，数据安全、云安全、SASE、终端安全等是主要收购的方向。
- 此外，部分安全龙头企业也在出售安全业务，其中McAfee出售企业安全业务，主攻个人安全业务。至此海外市场上已经没有“个人+企业”都经营的网络安全企业，而且包括McAfee在内，个人安全企业也只有两家。

全球主要公司近年来收购标的情况

企业	收购标的	业务内容	收购时间	企业	收购标的	业务内容	收购时间
Palo Alto	Demisto	以色列数据安全公司，业务侧重于安全工具编排和自动化安全技术	2019年	CrowdStrike	Humio	日志管理	2021年
	Puresec	美国云安全公司，主要产品为可信的安全计算环境中构建和维护安全可靠的无服务器应用	2019年		Cribl Inc	数据处理	2021年
	Twistlock	技术领先的容器安全企业	2019年		DoControl Inc	数据访问控制服务商	2021年
	Zingbox	物联网安全创业公司	2019年		Preempt Security	零信任网络安全	2019年
	Aporeto	云安全创业公司，分布式防火墙、身份识别代理和特权访问管理	2019年	Zscaler	Smokescreen Tech Pvt Ltd	欺骗、探测技术公司	2021年
	CloudGenix	全球领先的云交付厂商，SASE技术较强	2020年	飞塔	OPAQ Networks	零信任云解决方案	2020年
	Crypsis Group	终端安全企业，专注于事件响应、风险管理和数字取证	2020年		Panopta	SaaS平台、具备SASE能力	2020年
	Expanse	攻击面管理的安全初创公司，扫描企业IT资产提供漏洞监控服务	2020年	NortonLifeLock	Avast PLC	德国杀毒软件公司	2020年
	Sinefa	公司主要提供网络流量、终端监测等解决方案	2020年	Okta	Auth0	身份识别厂商	2021年
	Bridgecrew Inc	云安全公司，开创了“安全左移”的概念，将安全引入到开发环节	2021年	Akamai	Guardicore	零信任，微分段解决方案	2021年
Check Point	Avanan	为云电子邮件和 SaaS 协作套件提供安全保护	2021年	LG	Cybellum公司	汽车网络安全公司	2021年
	Forcenock Security	拥有一种基于机器学习算法的web应用程序和API保护（WAAP）技术	2020年	McAfee	Light Point	SASE	2020年

数据来源：bloomberg，平安证券研究所

目 录 CONTENTS

投资建议及风险提示

- **投资建议：**在我国数字化、智能化发展的大背景下，我国网络安全行业也面临着新的变革。线上化、云化提速让安全边界变得更为模糊；工业互联网和智能制造的发展也使得工控领域的安全风险持续暴露；产业数字化带来的数据资产快速积累，安全防护的重心也在向数据安全迁移。当前，我国网络安全监管进一步趋严，网络安全法律法规与行业标准正在密集出台，尤其是对新安全领域的防护，如数据安全等，要求更为严格。国内网络安全行业也正在顺应变化，加快产品研发投入，发力新安全领域。我国网络安全行业未来持续高景气发展可期。**强烈推荐启明星辰**，推荐**深信服、安恒信息和绿盟科技**。
- **风险提示：**1）竞争加剧的风险。随着数据安全等新安全市场的发展，不同背景的安全厂商同台竞争的可能性增大，比如互联网、传统ICT企业等，技术、品牌、人才和资金等方面的竞争加剧，行业总体和企业毛利率都存在下降的风险。2）技术风险加剧。数据安全作为新的安全领域，防护能力建设需要的是持续的研发投入，我国企业在新安全领域的研发同国际巨头还存在较大的差距，研发方向选择失误或者研发进度不及预期，都可能对企业短期业绩和长期发展带来不利影响。3）客户安全支出不及预期。行业客户多采用预算制进行产品和服务采购，宏观经济环境如出现不景气可能影响部分行业客户的IT投资预算。2021年以来，其他国家新冠疫情仍在蔓延，中美经贸关系也存在较大不确定性，国内经济增长仍面临较大压力，政企客户信息安全投入可能被迫下调或者推迟。

主要公司盈利预测及估值表

公司简称	证券代码	收盘价	EPS				PE				评级
		10/19	2020	2021E	2022E	2023E	2020	2021E	2022E	2023E	
启明星辰	002439.SZ	25.65	0.86	1.04	1.39	1.77	29.8	24.7	18.5	14.5	强烈推荐
深信服	300454.SZ	228.50	1.96	2.59	3.32	4.13	116.8	88.2	68.8	55.4	推荐
安恒信息	688023.SH	315.69	1.81	2.48	3.32	4.41	174.4	127.3	95.1	71.6	推荐
绿盟科技	300369.SZ	17.82	0.38	0.49	0.63	0.81	46.9	36.4	28.3	22.0	推荐

数据来源：Wind、平安证券研究所

股票投资评级：

强烈推荐（预计6个月内，股价表现强于市场表现20%以上）

推　　荐（预计6个月内，股价表现强于市场表现10%至20%之间）

中　　性（预计6个月内，股价表现相对市场表现在±10%之间）

回　　避（预计6个月内，股价表现弱于市场表现10%以上）

行业投资评级：

强于大市（预计6个月内，行业指数表现强于市场表现5%以上）

中　　性（预计6个月内，行业指数表现相对市场表现在±5%之间）

弱于大市（预计6个月内，行业指数表现弱于市场表现5%以上）

公司声明及风险提示：

负责撰写此报告的分析师（一人或多人）就本研究报告确认：本人具有中国证券业协会授予的证券投资咨询执业资格。

本公司研究报告是针对与公司签署服务协议的签约客户的专属研究产品，为该类客户进行投资决策时提供辅助和参考，双方对权利与义务均有严格约定。本公司研究报告仅提供给上述特定客户，并不面向公众发布。未经书面授权刊载或者转发的，本公司将采取维权措施追究其侵权责任。

证券市场是一个风险无时不在的市场。您在进行证券交易时存在赢利的可能，也存在亏损的风险。请您务必对此有清醒的认识，认真考虑是否进行证券交易。市场有风险，投资需谨慎。

免责条款：