西南证券
SOUTHWEST SECURITIES

计算机-网络安全行业专题报告

政策催化行业提速，估值有望进一步修复

西南证券研究发展中心
计算机研究团队
2022年12月

核心观点

- **网络安全是信息时代守护者，细分领域众多，全面覆盖重要行业。**网络安全是一种保护计算机网络免受入侵者攻击的技术，利用网络安全硬件、软件和网络安全服务针对中的病毒问题、非法访问和破坏、管理漏洞和网络缺陷及漏洞等对计算机系统硬件、软件和基础设施中的数据进行防御和保护。网按照“预防、防御、检测”三大纵深阶段划分，网络安全产品与服务可以分为数据安全、身份与访问安全、密码安全、防火墙、零信任等15个细分领域。我国网络安全客户主要集中在政府、教育、医疗卫生、公检司法和能源化工行业，这五个行业的客户数量占据了绝大部分的份额，其中政府行业客户数量最多。从客户数量增速来看，医疗卫生、教育、政府、党委和金融业的客户数量依然保持了较高的增长速度。

- **我国网络安全建设支出持续增长，5G安全、物联网安全、云安全等领域极具发展潜力。**2021年，《中华人民共和国个人信息保护法》发布，网络安全被提至战略新高度。随着国家在科技专项上的支持加大、用户需求扩大、企业产品逐步成熟和不断创新，网络安全产业依然处在快速成长阶段。近年来，受下游需求及政府政策的推动，我国网络安全企业数量不断增加，网络安全产业规模也不断发展。根据IDC数据，2021年我国网络安全市场支出约为819.9亿元，2022年预计达到993.7亿元。云存储、智慧化城市和5G三大应用场景的落地将会提高网络安全需求，我国网络安全投入占比未来将不断提升，根据IDC，预计2026年将增长至2144.2亿元，约占全球市场11.1%，市场空间广阔。随着我国云安全生态逐步形成，我国网络安全先进技术趋势出现变化，正由以硬件交付安全产品，人工交付安全服务的形式，逐步向云化、SaaS化方式交付技术和服务等形式转变。此外，随着零信任、XDR、隐私计算、安全开发等技术不断成熟，逐渐在实际场景中被采用和发挥效果，未来也将逐渐发展成为重要的网络安全技术架构。

- **主要标的：奇安信、深信服、信安世纪、安恒信息、永信至诚、信安世纪**

- **风险提示：**下游客户采购不及预期、行业政策不及预期、项目研发不及预期等风险。

目 录

1 网络安全客户采购驱动因素

2 网络安全行业发展趋势

3 网络安全核心细分领域

- 3.1 防火墙
- 3.2 数据安全
- 3.3 密码安全
- 3.4 身份与访问安全
- 3.5 零信任

4 网络安全行业国内外对比

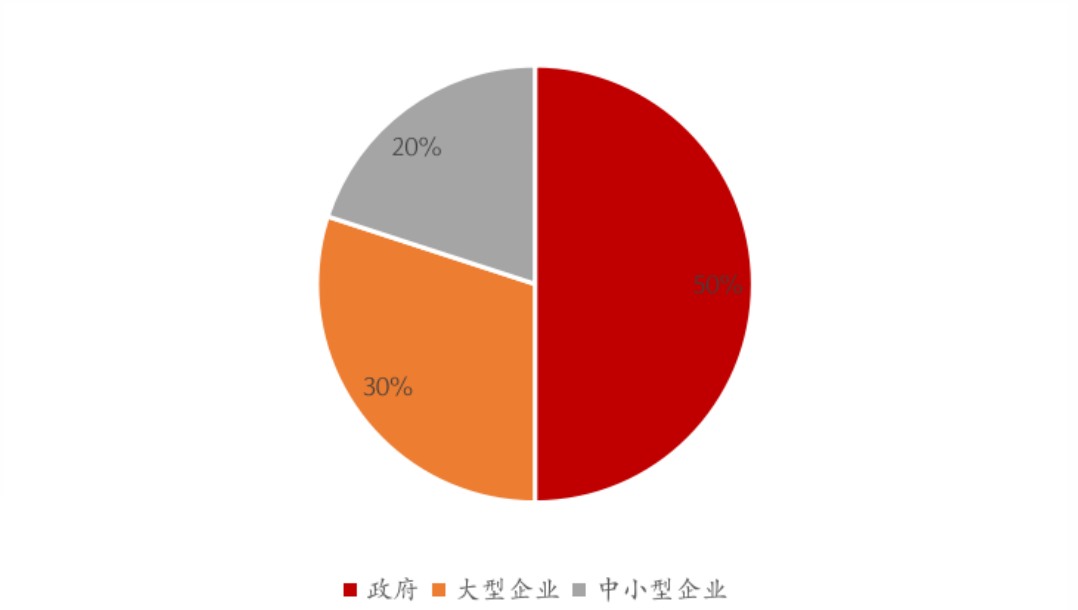
- 4.1 产业生态
- 4.2 竞争格局
- 4.3 人员构成

5 网络安全厂商未来核心竞争力

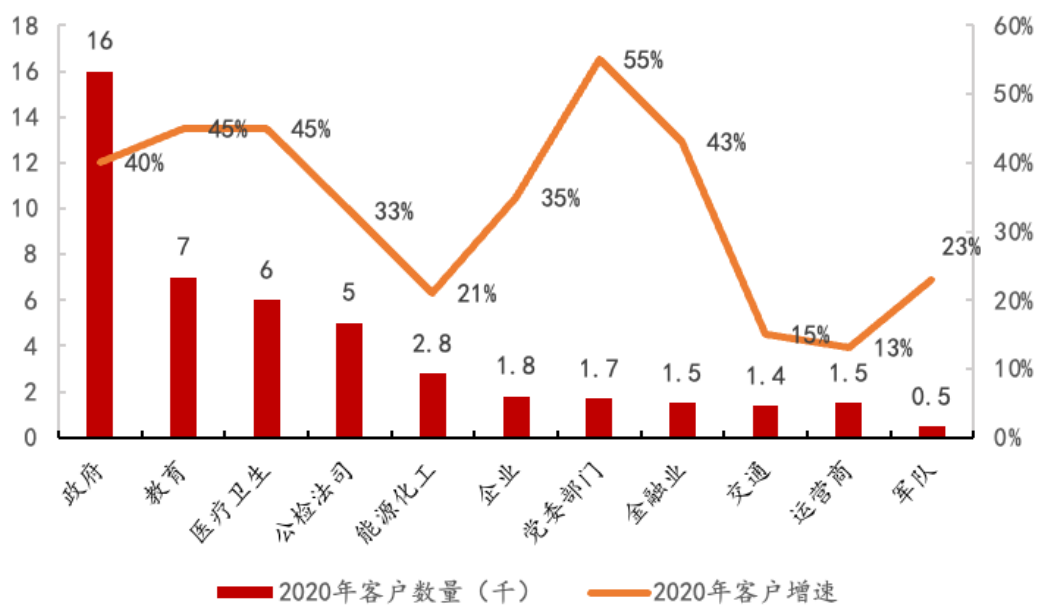
1 网络安全客户采购驱动因素

- **网络安全产品及服务**的**下游客户需求**由**性价比和产品力**驱动。**政府和中小型企业**在选购网络安全产品或服务更加**注重性价比**，而**大型企业**如金融、军工、国防、电信运营商在进行产品选择时更**偏重产品力**。
- **我国网络安全市场客户所属行业分布与行业的信息化水平强相关。**政府由于信息化开展较早，集中了大量的关键信息基础设施，网络安全防护需求强烈，目前是网络安全市场最主要的方向。**网络安全在政府客户数量占比达到50%，其次大型企业包括医疗卫生、教育、能源化工等行业客户数量占比达到30%，小型企业客户数量占比达到20%。**
- 2020年我国网络安全客户主要集中在**政府、教育、医疗卫生、公检司法和能源化工行业**，这五个行业的客户数量占据了绝大部分的份额，**其中政府行业客户数量最多。**从**客户数量增速**来看，**医疗卫生、教育、政府、党委和金融业的客户数量依然保持了较高的增长速度。**

网络安全公司客户占比



2020年中国网络安全市场客户行业分布及增速



数据来源：中国网络安全产业联盟，西南证券整理

1 网络安全客户采购驱动因素

政商关系驱动客户需求：

- **网络安全关乎国家、社会、政治安全，国资的引入加强了网络安全政策引导。**

目前，中国电科旗下已拥有**卫士通、绿盟科技、天融信**等3家网络安全板块上市公司。其中，卫士通偏重于密码领域，绿盟科技偏向于综合网络安全方向。2019年，**中国电子**以37.31亿元持有**奇安信**22.59%股份，**成为奇安信的第二大股东，而奇安信也变身为网络安全的“国家队”成员**。此外，**美亚柏科、数字认证**等网络安全公司均获得国资大手笔入股。

- **数字经济时代下，三大运营商与网络安全公司在技术和业务领域的协同效应正在持续显现。**

安恒信息与中国电信互为战略投资者，双方已建立了全面的**战略合作伙伴关系**，**中国电信**正全面实施**“云改数转”战略，以5G和云为核心打造云网融合的新型数字信息基础设施**。而**安恒信息**作为**国内领先的网络信息安全服务商**，在**应用安全、云安全、大数据安全、信创安全、物联网安全、智慧城市安全**等领域构筑了完善的产品线以及强大的技术优势。

国资入股网络安全公司的持股情况

	公司	持股比例	地位
中国电科	卫士通	36.0%	第一大股东
	绿盟科技	16%	第一大股东
	天融信	4.9%	第三大股东
中国电子	奇安信	22.6%	第二大股东
国资委	美柏亚科	15.6%	第二大股东
	数字认证	52.5%	第一大股东

三大运营商入股网络安全公司的持股情况

	公司	持股比例	地位
中国移动	启明星辰	23.1%	第一大股东
中国电信	安恒信息	2.7%	第七大股东
中国联通	云盾智慧	51.0%	第一大股东

数据来源：中国网络安全产业联盟，西南证券整理

1 网络安全客户采购驱动因素

价格差异化驱动客户需求：

- 从**短期**看，网络安全产品价格由**差异化价格**决定；**长期来看**，产品需求由综合实力决定，综合实力包含**产品资质以及功能的完善度。**在市场重新洗牌的再远期，产品定价主要依赖于**品牌，选择了好的品牌在一定水平上也就选择了好的技术和服务，对将来的使用更加有保障。**
- **绿盟创立时间早，品牌效应更加显著**，所以其**防火墙**产品**定价比天融信、深信服等网络安全产品更高。**对于**入侵检测**网络安全产品，**深信服产品价格要高于其它网络安全公司。**

下一代防火墙产品价格对比

设备类型	品牌	价格区间	产品数量
下一代防火墙	华为	2199元～16.3万	72
	绿盟科技	7.5万～60万	12
	天融信	1.5万～25.5万	16
	深信服	1.35万～27万	25
	思科	3900元～6.5万	17

入侵检测产品价格对比

设备类型	品牌	价格区间	产品数量
入侵检测	华为	11.86万～19.8万	2
	绿盟科技	9.3万～35万	7
	天融信	16万～41万	3
	深信服	30万～54.2万	2
	网御星云	13.8万～26.8万	5

数据来源：中国网络安全产业联盟，西南证券整理

1 网络安全客户采购驱动因素

合规要求驱动客户购买网络安全产品及服务：

- **网络安全法律法规体系不断完善**，相关配套制度加速落地，网络安全标准体系进一步完善，**推动网络安全需求侧持续加大安全投入，促进网络安全需求加快释放，网络安全产业发展迎来新契机。**
- 近年来，我国政府颁布了新的**《国家安全法》、《网络安全法》**等重要法规并制定了**《“十三五”国家信息化规划》、《软件和信息技术服务业发展规划（2016 - 2020）年》、《信息通信网络与信息安全规划（2016-2020）年》**等政策，从**制度、法规、政策**等多个层面促进国内网络信息安全产业的发展，**提高对政府、企业等网络信息安全的合规要求。**

网络安全行业相关法律法规

发布时间	发文单位	法律法规名称	相关内容概要
2017年	工信部	《公共互联网网络安全威胁监测与处置办法》	积极应对严峻复杂的网络安全形势，进一步**健全公共互联网网络安全威胁监测与处置机制**，维护公民、法人和其他组织的合法权益。
2017年	中央网信办	《网络产品和服务安全审查办法（试行）》	为**提高网络产品和服务安全可控水平**，防范供应链安全风险，维护国家安全和公共利益制定。
2017年	工信部	《公共互联网网络安全威胁监测与处置办法》	积极应对严峻复杂的网络安全形势，进一步**健全公共互联网网络安全威胁监测与处置机制**，维护公民、法人和其他组织的合法权益。
2017年	工信部	《公共互联网网络安全突发事件应急预案》	**建立健全公共互联网网络安全突发事件应急组织体系和工作机制，提高公共互联网网络安全突发事件综合应对能力，**确保及时有效地控制、减轻和消除公共互联网网络安全突发事件造成的社会危害和损失，保证公共互联网持续稳定运行和数据安全，维护国家网络空间安全，保障经济运行和社会秩序。
2017年	中央网信办	《国家网络安全事件应急预案》	建立健全国家网络安全事件应急工作机制，**提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、**公共安全和社会秩序。
2016年	工信部	《互联网信息安全管理系统使用及运行维护管理办法（试行）》	指导各省、自治区、直辖市通信管理局以及经营互联网数据中心（含互联网资源协作服务）、互联网接入服务、内容分发网络服务等业务的互联网接入类企业规范**做好互联网信息安全管理系统的使用与运行维护管理工作；保障各单位系统安全可靠运行**，有效发挥系统作用。
2014年	中央网信办	《关于加强党政机关网站安全管理的通知》	**各地区各部门在规划建设党政机关网站**时，应按照同步规划、同步建设、同步运行的要求，参照国家有关标准规范，从业务需求出发，**建立以网页防篡改、域名防劫持、网站防攻击以及密码技术、身份认证、访问控制、安全审计等为主要措施的网站安全防护体系**。切实落实信息安全等级保护等制度要求。
2014年	工信部	《关于加强电信和互联网行业网络安全工作的指导意见》	**加大对基础电信企业的网络安全监督检查和考核力度**，加强对互联网域名注册管理和服务机构以及增值电信企业的网络安全监管，推动建立电信和互联网行业网络安全认证体系。

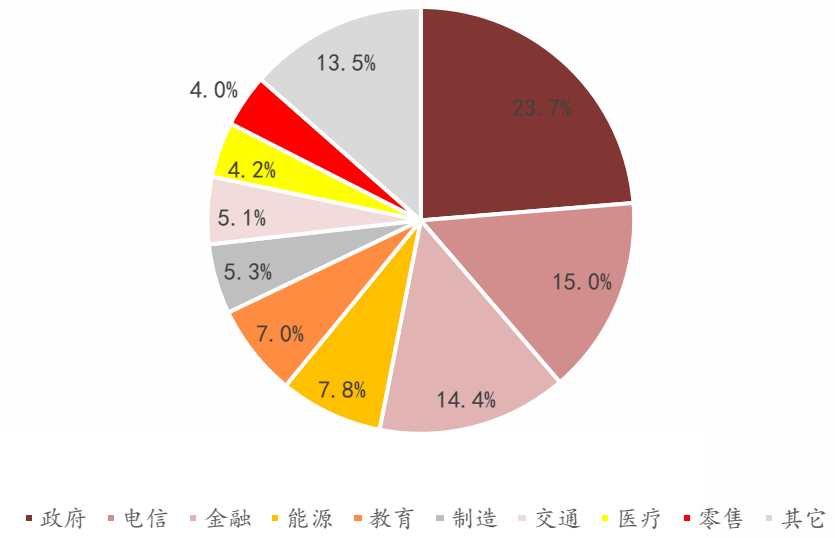
信息来源：中国网络安全产业联盟，西南证券整理

1 网络安全客户采购驱动因素

自身防御需求驱动客户购买网络安全产品及服务：

- **下游终端客户**的需求者主要为**信息化程度较高且对信息较为敏感的行业**，包括**政府部门、军队、金融行业、电信行业、能源行业、教育行业**等。在我国，以**电信、金融、能源**等为代表的重点行业事关国家经济稳定与社会发展。在为满足国家监管要求的同时，由于其业务发展迅速，为提高自身的行业竞争力，这些行业内的企业纷纷选择**信息化手段**来提高其管理水平与竞争优势，**这些重点行业信息化建设投资的不断增加将为网络信息安全行业的发展创造出新的市场空间。**
- **大数据时代，各行业都避免不了不同程度上的黑客攻击**，安全防护可以说已经成为了一个全“业”运动。但虽然领域不同，行业不同，具体的防护需求也都不尽相同，但是归根结底，**最深层、最根本的方向是一样的**，那就是**保证信息本源的安全。**

中国网络安全行业应用市场占比情况



三大行业网络安全需求

行业	安全需求
电信	确保**核心信息与资源的保密性、完整性和可用性**。在保障用户利益、体验和隐私的基础上充分发挥数据价值。
金融	**对访问控制、处理算法、网络安全、数据管理和应用等方面提出安全要求，**期望利用大数据安全技术加强金融机构的内部控制，提高金融监管和服务水平，防范和化解金融风险。
政府	隐私保护的安全监管、网络环境的安全感知、大数据安全标准的制定、安全管理机制的规范等内容。

数据来源：中国网络安全产业联盟，西南证券整理

目 录

1 网络安全客户采购驱动因素

2 网络安全行业发展趋势

3 网络安全核心细分领域

3.1 防火墙
3.2 数据安全
3.3 密码安全
3.4 身份与访问安全
3.5 零信任

4 网络安全行业国内外对比

4.1 产业生态
4.2 竞争格局
4.3 人员构成

5 网络安全厂商未来核心竞争力

2 网络安全行业发展趋势—现状

从多个分析维度和数据来源看，**我国网络安全投资在信息化投资中的占比与世界平均水平相比有1至2倍的差距，与美国相比差距更为显著。**

- 根据Gartner的数据测算，我国网络安全在IT总投入中的占比2016年为**0.8%**、2017年为0.9%。对照全球平均水平，根据IDC数据，**我国网络安全在IT总投入中的占比与全球平均数据相比存在约1.8倍的差距（2016年和2017年我国的投入占比均约为全球平均水平的35%）**，与美欧等领先国家相比，差距更加明显。当前，美欧在重要IT系统建设中的网络安全投入占比达到15%~25%。美国特朗普政府提出的2018年度联邦政府预算中，网络安全的投入在IT总投入中的占比达到了20%。
- **网络安全意识薄弱、网络安全责任落实不到位、网络安全工作科学理念普及率低下**是导致投入不足的主要原因。**总体投入不足**是我国网络安全产业发展生态环境建设急需解决的关键性问题。

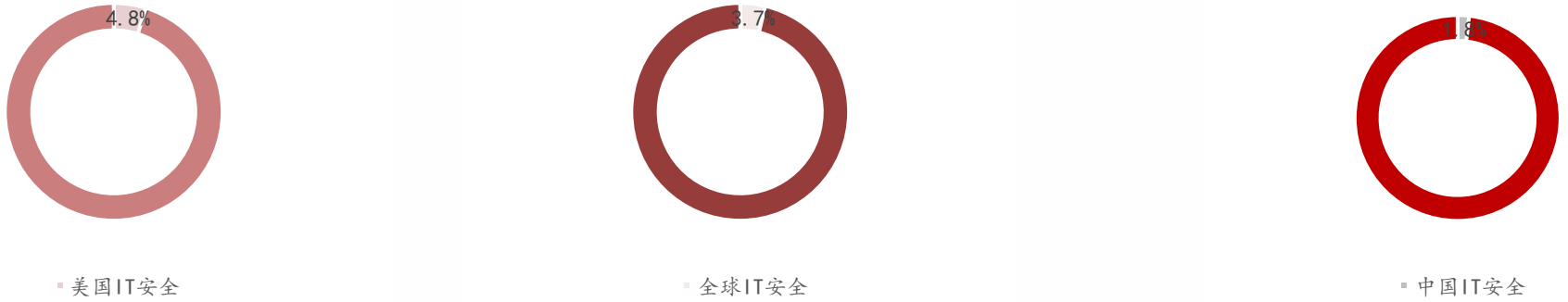
中国网络安全投入在IT总支出中的占比

年份	中国网络安全支出（亿美元）	中国IT总支出（亿美元）	占比
2016	27.4	2.22	0.8%
2017	31.7	2.34	0.9%

全球网络安全投入在IT总支出中的占比

年份	全球网络安全支出（亿美元）	全球IT总支出（亿美元）	占比
2016	33960	807	2.4%
2017	35270	864	2.5%

IT安全占IT市场比例的对比



数据来源：IDC公司，Gartner，西南证券整理

2 网络安全行业发展趋势—未来趋势

云存储、智慧化城市和5G三大应用场景的落地将会提高网络安全需求，我国网络安全投入占比未来将不断提升

- **1.云存储业务将扩大数据安全投入占比**

  纵观全球，中国的IT建设是比较超前的。中国数据中心存储用量、云存储占全球的比例是20%，但云存储安全投入占全球4%-5%。**中国云存储业务将驱动对网络安全产品和服务的需求**，未来，数据安全在网络安全整体市场中将占到适当的份额，根据信通院数据，**2023年我国数据安全市场规模可达97.5亿元，占网络安全市场比重提升至12.1%。**

- **2.智慧化城市的发展将促进网络安全业务的投入**

  中国智慧城市的建设连续数年每年投资1万亿元。政府，包括5G结合智慧城市均将实现数字化，从而安全比重也会提升。相比于传统合规市场，**智慧城市市场规模潜力巨大。**由于智慧城市属于**集成建设**，所以**对IT公司的综合实力要求较高**，从而**为实力雄厚的IT公司**比如说东软、浪潮**提供了巨大的发展契机。**

- **3.5G的发展驱动了网络安全业务的投入**

  5G规模也很大，运营商2020年已经完成了地市和所有省市的覆盖，预计今年完成5G建设。







数据来源：中国网络安全产业联盟，信通院，西南证券整理

2 网络安全行业发展趋势—未来趋势

未来国内投入占比会提升，但进度比较慢，主要基于以下原因：

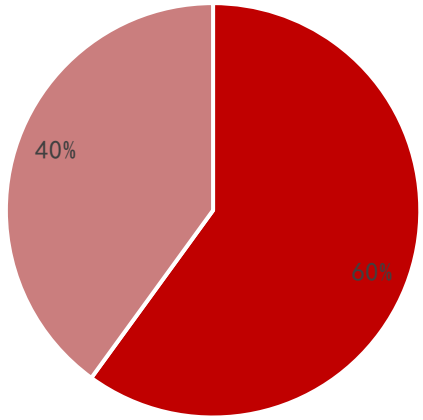
- **我国政策落地较为复杂，**在政策执行层面，考虑各地执行有差异，所以政策落地总体进度不及预期。此外，大数据是2020年左右才陆续开始建立的，伴随着机构改革，**收集各个省市的经济数据速度较慢，再加上业务迁徙，政策真正落地时间较长。**
- **财政支出缩紧会影响网络安全业务收入**，网安公司一般前**三个季度收入占比60%，剩下40%的收入在第四季度产生。**

网络信息安全行业的主要客户对象为政府机构、电信运营商、金融、教育、能源等领域内的公司，这些客户受预算体制和采购习惯的影响，通常在上**半年进行预算管理，制订采购计划，在下半年进行采购和付款。**因此，**网络信息安全行业内各公司在下半年实现的收入占比较高，收入具有一定的季节性。**

政策落地流程



网络安全公司营业收入季度占比





数据来源：中国网络安全产业联盟，西南证券整理

目 录

1 网络安全客户采购驱动因素

2 网络安全行业发展趋势

3 网络安全核心细分领域

3.1 防火墙
3.2 数据安全
3.3 密码安全
3.4 身份与访问安全
3.5 零信任

4 网络安全行业国内外对比

4.1 产业生态
4.2 竞争格局
4.3人员构成

5 网络安全厂商未来核心竞争力

3.1 防火墙——定义

- **防火墙的定义**：（1）对相关的网络信息**进行防范过滤**；（2）**保证内网、外网对外通信的流畅，防止不法侵害内容渗入；（3）**主要对内部起到**保护性作用的屏障。**
- **防火墙的演进脉络**：其一，**在顺应着带宽、应用、流量的发展背景下**，整个网络应用环境繁荣，不断地给防火墙提出新要求，**防火墙需求脉络推动着防火墙演技脉络的发展**；其二，**随着5G带宽更宽，整个部署环境变化很大（如：企业上云、政务云），始终对一个静态边界或者网关设置有所需求**，由此推动了防火墙的发展。

防火墙发展流程

中国防火墙最早大概是90年代初**天融信**在做，大量企业在2000年前后成立。

包过滤的防火墙

由于带宽小，**防火墙会对每个报文做检查以及对每个包过滤，这是第一代防火墙设置的SR规则（复制访问规则）。**第一代防火墙功能比较简单，性能较低，很多现代的技术都没用上。

代理防火墙

在2000年前后出现，**国内代表性的企业包括天融信、启明和华为等**都是做这一代，国际上主要是Cisco、Checkpoint这些公司在做。**第二代是有一个状态相当于门，规则是动态的，只要来过一次就会记住，下次无需防护。**

下一代防火墙 NGFIREWALL 帕拉特提（2007）

在那时，web2.0整个应用爆炸，外加3G带宽与之前不同，应用也越来越多。**第三代防火墙相当于做了一个深度识别，特点就是用户识别和应用识别。**

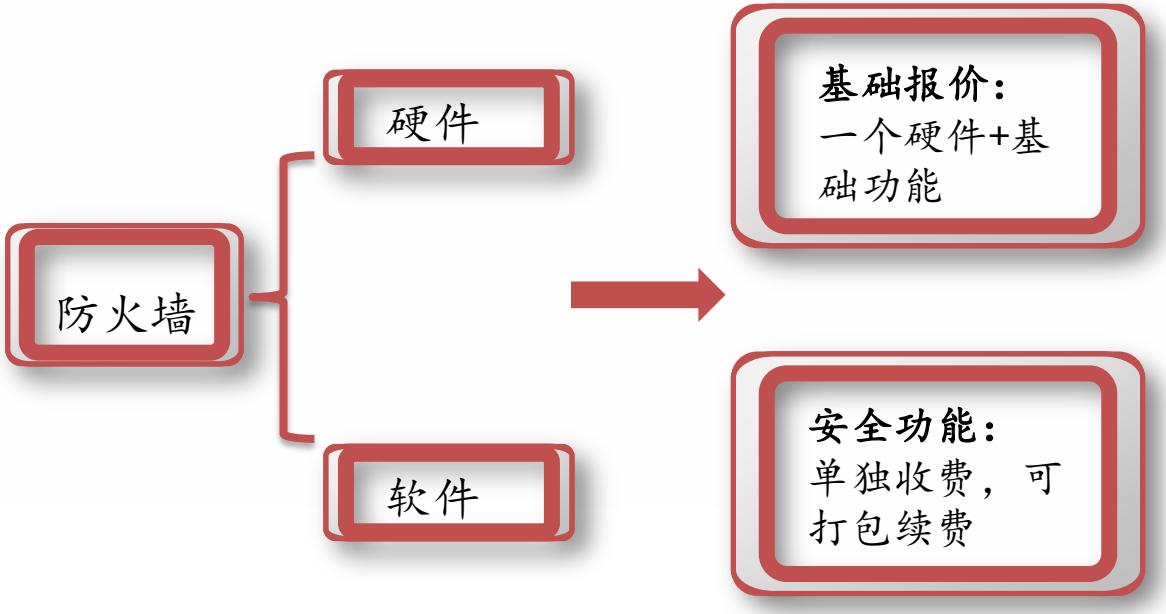
下一代防火墙增加了深度的报文检测，具体而言是它会**先深度识别用户和报文的内容再过滤**，较于以前，过滤得地更加精细，更贴合用户的应用。

信息来源：中关村在线，西南证券整理

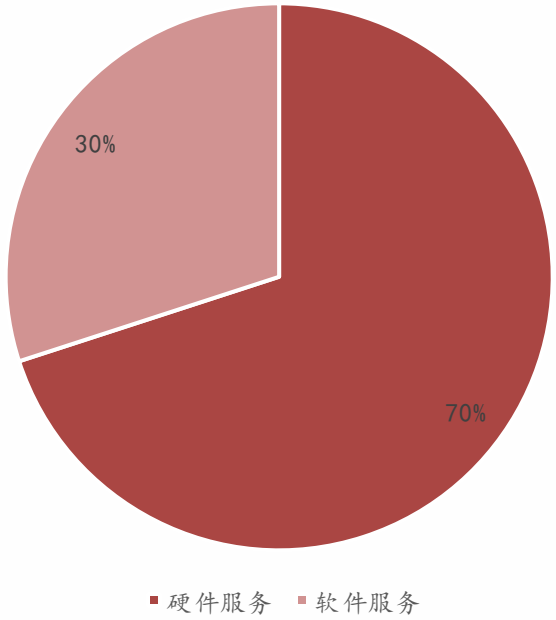
3.1 防火墙——采购周期

- **防火墙生命周期大概是5年**
- 在进行**防火墙采购过程**中，其相关的**硬件和软件是需要分开采购。**最开始可以先买**一个硬件加基础功能，这套称为基础报价，而安全功能是单独收费的**，可以按年或三年期限进行打包续费。
- **在购买软件服务之后，可以根据规则操作按周、按月定期升级，持续升级，在售后上具有保障性。**例如，产生了一个新的攻击，安全厂商可能会在24小时内开发出对应的应急响应包发布，用户只需要升级即可。
- 厂商的销售模式**通常是硬件、软件一起卖，**并提供相应服务。其中**硬件占厂商总收入的大概比例为百分之六七十，软件续费lisence大概占厂商总收入的大概比例为百分之三四十。**

防火墙采购模式



厂商收入占比构成



数据来源：安全牛，西南证券整理

3.1 防火墙——技术衡量指标

硬件设计能力和**软件设计能力**是决定一个防火墙性能好坏的关键。

- **硬件能力主要体现在通讯能力和安全性能两个核心指标上。**传统数通厂商积累较好，比如华为、山石、华三等企业做数据通信发家，有硬件设计能力，通过给防火墙加交换板卡，进而提升防火墙的性能。相同的硬件成本下，这类厂商的产品性能比其他厂商性能更高。其他传统网络安全厂商硬件能力较弱，诸如启明星辰和绿盟等企业目前还是在买现成硬件。所以在大带宽的场景下，比如运营商视频、云商环境等，硬件能力弱的企业无法进入这类市场，只有传统的第一梯队企业可以进去。
- **软件能力主要体现在安全引擎中规则数量和规则更新频率两个指标上。**防火墙里中的安全引擎是一个规则库，引擎是通用的。安全公司的竞争力在规则数量，新出一个攻击，需要有新的规则才能继续保护，所以主要是靠加载在引擎上的规则，不停升级规则。防火墙有杀病毒的规则库，有入侵检测的规则库，有行为识别的规则库，在出售时会在一个时间点安装一个基础的规则库，后续会在上面叠加。规则更新一般有两条路径：（1）在线升级，可联网时，直接连接厂商的升级网站升级防火墙；（2）现场升级，如果无法联网，服务人员可以用U盘将新的规则拷贝，去客户现场升级。

网络安全厂商硬件能力对比

传统数通厂商

HUAWEI　Hillstone 山石网科　H3C

- 数据通信发家，有硬件设计能力；
- 通过给防火墙加交换板卡，类似于FPGA板卡进而提升很大性能。
- 相同的硬件成本下，这类厂商会比在这方面技术更差的厂商性能更高。

传统网络安全厂商

启明星辰　NSFOCUS 绿盟科技

- 硬件能力较弱
- 外采硬件
- 在大带宽的场景下，硬件能力弱的企业无法进入防火墙市场

信息来源：CSDN，西南证券整理

3.1 防火墙——云化部署

防火墙云化部署有三大技术要求：

1. **防火墙有足够弹性：**云本身是弹性的，所以在云端的软件化部署，根据流量不断增长，防火墙也需要足够弹性；
2. **改造硬件防火墙适配虚拟化的网络：**云端部署形态是虚拟化的，网络也是虚拟化的，硬件防火墙需要做一些改造来重新适配虚拟化的网络；
3. **改造增值运营的商业开通、计费模式：**云上模式和线下卖硬件的增值运营要求不一样，云上服务可以只买一个月不复购，但线下硬件是不行的，购买硬件只有就必须得用，因此需要对增值运营的商业开通、计费模式做一些改造。

互联网边界防火墙和主机边界防火墙原理图

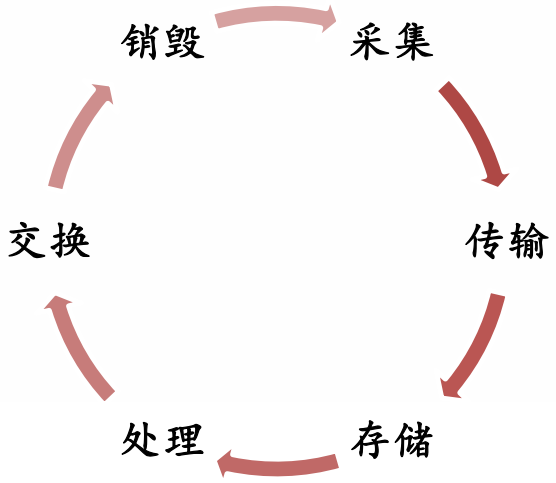


信息来源：阿里云，西南证券整理

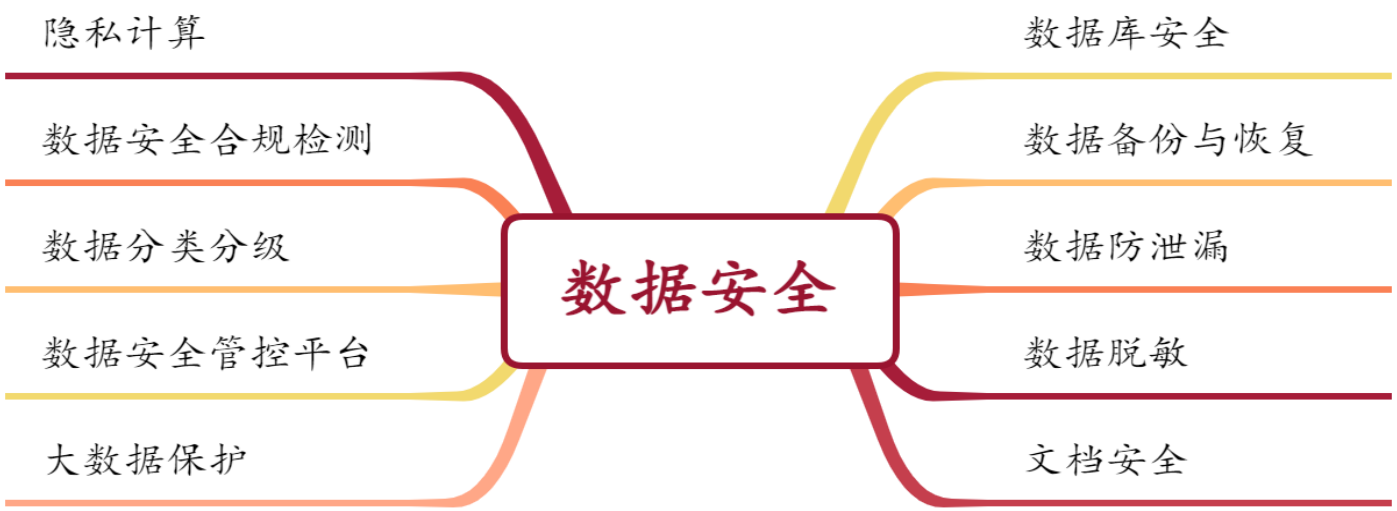
3.2 数据安全——定义

- **数据安全（DataSecurity）**：原指数据库安全和内部数据防泄漏。随着网络结构不断复杂化，数据安全现指以数据为中心的安全体系，以数据的采集、传输、存储、处理（使用）、交换（共享）、销毁等覆盖全生命周期的安全为目标，侧重于从数据产生到销毁的全生命周期的保护，保护方式类似于伴随数据全生命周期的安保人员，强调数据的所有权、管辖权、隐私权等。
- 根据安全牛发布的《中国网络安全行业全景图（第九版）》，**数据安全涉及数据库安全、数据备份与恢复、数据防泄漏、数据脱敏、文档安全、大数据保护、数据安全管控平台、数据分类分级、数据安全合规检测和隐私计算等10大细分领域。**
- 过去，我国数据安全建设包含在网络安全的建设之中，以满足等级保护规范要求为主要标准，围绕数据库保护数据防泄漏、数据脱敏等展开。2019年，等保2.0相关国家标准正式发布，安全要求拓展为安全通用要求和安全拓展要求，针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护基本要求标准，数据安全保护要求更加严格。

数据生命周期



数据安全细分领域



信息来源：数说安全，安全牛，西南证券整理

3.2 数据安全——重要产品

数据安全领域重要产品

产品名称	简介	领域
华控清交多方安全计算平台PrivPy	PrivPy多方安全计算平台实现了支持通用计算类型、高性能、集群化和可扩展的解决方案。支持标准的Python语言和SQL操作，兼容NumPy和Pytorch等函数库，能够支持包括绝大多数机器学习算法在内的计算类型和系统实现，极大的降低了用户使用密文计算的学习曲线，实现了多方安全计算产品的实际可用性和商业易用性。同时，PrivPy自主灵活的模块化组合模式和多种部署方式能够满足广泛用户群体在使用和部署中的多样化需求。	隐私计算
阿里云数据库审计	在满足等保2.0‘安全审计’相关要求的同时，智能解析数据库通信流量，细粒度审计数据库访问行为，通过对数据库全量行为的审计溯源、危险攻击的实时告警、风险语句的智能预警，提供敏感的数据库资产最安全的监控保障	数据安全合规监测
安恒AiSort数据安全分级及风险管理平台	能够对用户数据进行自动发现和分类分级。产品基于AI算法实现对敏感数据准确高效识别，内置多行业的法规标准（支持自定义导入）满足多种环境下的分类分级需求。系统支持对用户数据资产进行漏洞评估、安全风险评估，帮助用户从多个维度感知数据资产安全状况。	数据分类分级
天融信数据安全智能管控平台	天融信数据安全智能管控平台通过可视化视图全面掌握用户数据库、存储系统，从数据维度获取数据资产情况，针对性发现相关敏感数据并对其进行分类分级，从安全角度梳理数据资产，满足符合行业法规的要求。通过数据流向的地图化展示，有效监控敏感数据的流向，提供数据标签策略、策略基线以及策略版本的全面数据安全策略管理，结合数据资产信息、数据行为审计信息，通过多种数据分析模型，实现数据多维度展示及数据流转中的态势呈现和风险识别，并且提供统计分析报表的能力。	数据安全管控平台
深信服太衍大数据平台	深信服太衍大数据平台支持各种异构数据源的连接，实现多种数据类型数据数据采集和数据标准化在大数据平台中进行统一的数据集中存储和分析。深信服大数据平台提供极简的低代码开发平台，有效降低了开发难度，为上层的应用开发工作提供了稳定高性能的基础平台，大数据强大的算力为业务持续不断稳定的运行保驾护航。大数据平台从功能分为了大数据技术支撑平台Base和大数据智能开发平台Studio	大数据保护
阿里云数据安全中心	为客户提供敏感数据自动识别、分级分类、大数据安全审计与数据脱敏等数据安全能力，形成一体化的云上全域数据防泄漏与安全解决方案，在帮助客户实现等保2.0二级有关“安全审计”与三级有关“个人信息保护”的合规要求的同时，并满足《数据安全法》中提出的有关要求。	数据库安全 数据脱敏
奇安信数据脱敏系统	奇安信网神数据静态脱敏系统是将生产环境中的真实数据“搬移并仿真替换”处理后，下发给下游环节，随意取用和读写的，脱敏后数据与生产环境相隔离。满足企业数据自身使用、外发分析等需求的同时保护敏感数据不被泄露的数据安全专用设备。	数据脱敏
奇安信网神数据防泄漏系统	奇安信网神数据防泄漏系统遵循以数据为中心的安全架构设计，使用先进分类分级数据内容识别引擎，结合用户行为分析技术，覆盖网络终端、邮件、存储等关键位置，完美解决数据分布集中展示、敏感数据使用、敏感数据传输风险预警、用户行为预警的难题。客户能够借助产品中数据分类能力，实时梳理不同业务类别数据，实现可视化展现和差异化分类保护策略。	数据防泄漏
启明星辰铁卷数据安全系统	铁卷数据安全系统是一款以透明加密技术为核心的电子文档安全产品，它能够帮助用户保护知识产权、提升企业形象和核心竞争力。它能够帮管理者实现：电子文档加密；操作日志审计；外发文档防护。铁卷数据安全系统从电子文档的产生开始即对文档进行防护，对文档的操作、拷贝、传输、打印、外发、删除建立了全程的保护体系。	文档安全

信息来源：华控清交、阿里云、安恒信息、天融信、深信服、奇安信、启明星辰公司官网，西南证券整理

3.2 数据安全——法律法规

近年来，政策规划不断加强对数字经济和数据要素的指导及要求，数据要素和数字经济的重要性不断提升。

- 2021年12月国务院印发《**“十四五”数字经济发展规划**》，指出数据作为数字经济时代下的基础性资源和战略性资源，是决定国家经济发展水平和竞争力的核心驱动力。**发展数字经济正式上升为国家重要发展战略，数据安全则成为保障数字经济健康发展的重要基石。**作为国民经济和社会发展的风向标，**“十四五”规划和2035年远景目标纲要**里，**数据安全建设融入到各个篇章中**，对建设数字化中国和打造网络安全强国做出了重要部署。
- 近年来，数据安全标准体系加速建立，各行业、地方的数据安全标准规范密集落地，数据安全足部迈入强监管阶段。**2021年6月10日《数据安全法》颁布，重新改写了数据安全的定义，标志着数据安全新时代的到来。**

十四五规划纲要数据安全相关内容

章节		相关内容
第十五章	打造数据经济新优势	充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合
第十七章	提高数字政府建设水平	将数字技术广泛应用于政府管理服务，推动政府治理流程再造和模式优化
第十八章	营造良好数字生态	坚持放管并重，促进发展与规范管理相统一，构建数字规则体系，营造开放、健康、安全的数字生态
第二十章	建设高标准市场体系	发展技术和数据要素市场。健全要素市场运行机制，完善交易规则和服务体系。深化公共资源交易平台整合共享
第五十二章	加强国家安全体系和能力建设	全面加强网络安全保障体系和能力建设，切实维护新型领域安全

部分行业数据安全标准规范

电信行业	《基础电信企业数据分类分级方法》	《基础电信企业重要数据识别指南》	《电信和互联网行业数据安全标准体系建设指南》
	《电信运营商大数据安全管控分类分级技术要求》	《电信网和互联网数据安全通用要求》	《电信网数据泄露防护系统(DLP)技术要求》
	《电信大数据平台数据脱敏实施方法》	《电信网和互联网数据安全评估实施技术要求》	《电信网和互联网数据安全风险评估实施方法》
	《电信网和互联网数据安全评估规范》	《电信运营维护管理数据的管理技术要求》	.....
金融行业	《金融数据安全分级指南》	《金融大数据术语》	《金融业数据能力建设指引》
	《个人金融信息保护技术规范》	《证券期货业数据分类分级指引》	《金融数据安全数据生命周期安全规范》
	《金融大数据平台总体技术要求》	《金融数据安全评估规范（征求意见稿）》	《保险行业信息共享平台数据交换规范》
	《中国银保监会监管数据安全管理办法（试行）》	《数字函证银行应用数据规范》	.....
政府行业	《政务服务平台基础数据规范》	《政务服务平台接入规范》	《信息安全技术个人信息去标识化指南》
	《政务数据分类分级规范/指南》	《公共安全大数据数据采集与预处理》	《信息安全技术个人信息安全规范》
	《信息技术大数据政务数据开放共享》	《基于云计算的电子政务公共平台服务规范》	《信息安全技术政务信息共享数据安全技术要求》
	《政务数据平台第3部分：数据存储规范》	《信息安全技术数据交易服务安全要求》	.....

信息来源：数说安全，西南证券整理

3.2 数据安全——治理体系

数据安全价值

安全合规要求应对

《数据安全法》中强调了对重要数据的保护，明晰了数据分类分级保护制度；《个人信息保护法》中明确规定个人信息应当实行分类管理；《中国银保监会监管数据安全管理办法(试行)》规定采取分级分类安全技术防护措施应对监管数据类型和管理要求；《医疗卫生机构网络安全管理办法》规定各医疗卫生机构需对每年数据资产梳理。

提高业务安全强度

识别敏感数据，并掌握组织敏感数据中资产分类、分级、分布情况及各类数据的使用场景。
制定高校防护措施，降低各项业务的安全风险，平衡数据流动创造价值与数据安全的矛盾。
精细化管控数据资产，有效性监控敏感数据，“可见可控”化据使用、数据共享行为。

提升自身业务能力

数据资产清单能促使组织业务的良性持续发展，提升数据质量，帮助业务部门在进行相关性数据处理场景时，提供更为有效合理的策略，进而提升业务运营能力，为组织带来精准的数据服务。

数据安全治理框架

序号	过程类	过程域
1	数据采集安全	P1数据分类分级
2		P2数据采集安全管理
3		P3数据源鉴别及记录
4		P4数据质量监控
5	数据传输安全	P5数据传输加密
6		P6网络可用性管理
7	数据存储安全	P7存储媒体安全
8		P8逻辑存储安全
9		P9数据备份和恢复
10	数据使用安全	P10数据脱敏
11		P11数据分析安全
12		P12数据正当使用
13		P13数据处理环境安全
14		P14数据导入导出安全
15	数据交换安全	P15数据共享安全
16		P16数据发布安全
17		P17数据接口安全
18	数据销毁安全	P18数据销毁处置
19		P19存储媒体销毁处置
20	通用安全过程域	P20数据安全策略规划
21		P21组织和人员管理
22		P22合规管理
23		P23数据资产管理
24		P24数据供应链安全
25		P25元数据管理
26		P26终端数据安全
27		P27监控与审计
28		P28鉴别与访问控制
29		P29需求分析
30		P30安全事件应急

信息来源：好大夫，西南证券整理

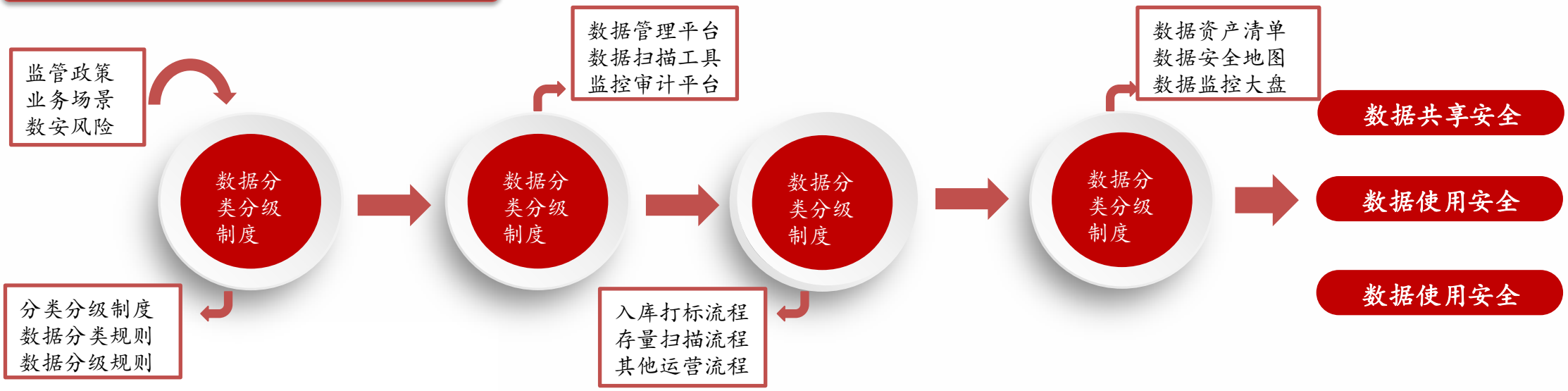
3.2 数据安全——数字分类分级工作

数据安全应用场景

监管合规要求
法律法规、行业监管要求国标、行标、指南等
业务系统场景
APP、PC站站主要业务功能如何开展、如何采集的数据
数据安全风险
数据水平越权、数据过度暴露、数据使用不合规等

外部最佳实践
行业头部企业最佳实践
数据使用场景
内/外部使用场景、业务方使用场景、委托处理场景
数据安全事件
企业已发生或可感知到的数据安全事件(泄露、通报等)

数据安全分级思路框架



信息来源：好大夫，西南证券整理

3.2 数据安全——分级制度建设

示例数据分类分级建设

1. 在《信息安全技术健康医疗数据安全指南》基础，结合互联网医疗现有业务场景，制定了《XXX数据分类分级规范》。

2. 把线上业务数据字段分为个人属性数据、身份鉴权数据、健康相关数据、医疗应用数据、医疗支付数据和其他6类4个级别。

3. 根据数据分类分级规范细化制定各类数据安全规范，规范主要是针对各类数据安全关键管理活动。

数据分类分级建设

层级	类型	序号	制度名称
一级	方针	L1-001	XXX数据安全管理策略
二级	制度	L2-001	XXX数据安全生命周期管理制度
三级	规范	L3-001	XXX数据安全规范 数据分类分级
	规范	L3-002	XXX数据安全规范 业务安全合规评估
	规范	L3-003	XXX数据安全规范 权限管理
	规范	L3-004	XXX数据安全规范 合作方安全管理
	规范	L3-005	XXX数据安全规范 安全审计
	规范	L3-006	XXX数据安全规范 数据备份
	规范	L3-007	XXX数据安全规范 应急响应
	规范	L3-008	XXX数据安全规范 安全教育培训
	规范	L3-009	XXX数据安全规范 投诉管理

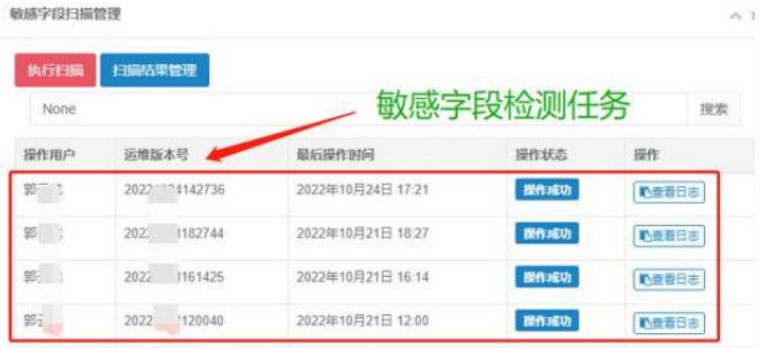
信息来源：好大夫，西南证券整理

3.2 数据安全——数据分类分级工具

1数据安全管理平台

数据分类分级管理功能：
资产清单呈现、分类分级打标、检测任务管理

➢ **数据安全管理平台**



2敏感数据识别工具

目前使用开源软件D18N，D18N是一款强大的**数据脱敏**和**敏感数据**识别工具

与数据安全管理平台集成：
1、创建控制扫描任务(定时)
2、扫描结果自动比对(去重)
3、扫描结果人工确认(3/4级确认)

D18N工具支持识别规则：
1、正则表达式匹配(字段命名规范)
2、关键字规则匹配(业务数据特点)
3、自然语言处理包(姓名、地址)

➢ **D18N工具支持识别**



3数据安全大盘

技术团队使用了**grafana可对接MySQL、ClickHouse、Elasticsearch三个系统数据源**，可展示和监控的各类动静态数据主要展示数据分类分级情况、敏感数据字段分布、各类数据使用活动监控、第三方使用敏感数据情况等。

➢ **数据安全大盘**



信息来源：好大夫，西南证券整理

3.2 数据安全——分类分级难点坑点

数据分类分级难点坑点

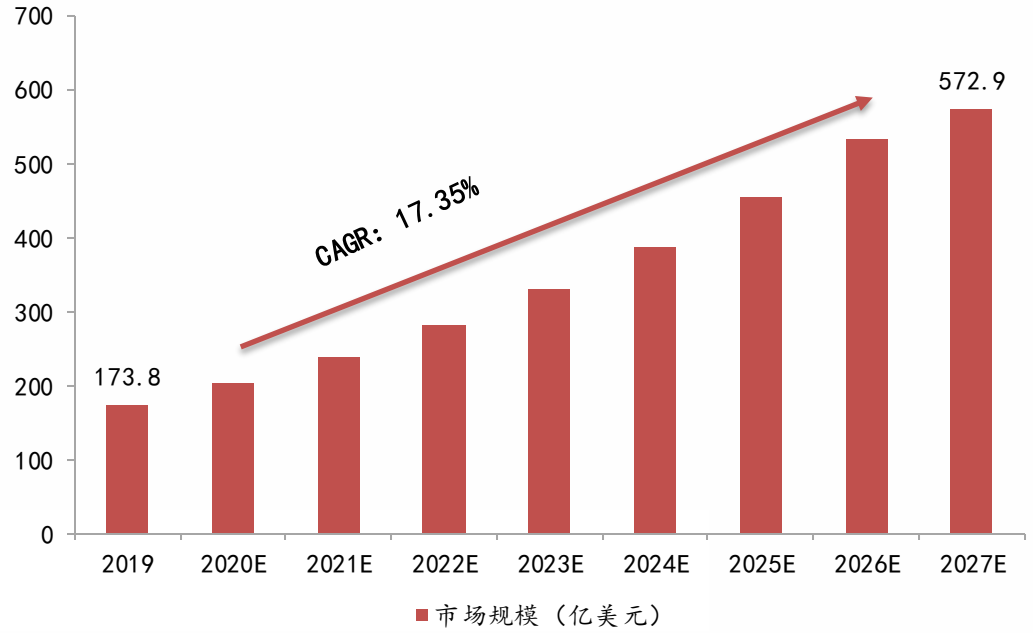
难点坑点	详细阐述
数据安全相关规范的持续迭代	建设初期各项规范一定是相对宽泛，随着数据安全分类分级推进成熟，各类规范也应当持续更新和及时的宣贯，保证流程的规范性和延续性。
MongoDB数据库敏感数据识别	MongoDB不能直接使用扫描工具扫描，需要使用官方BIConnector，该组件提供能力使客户端可以通过SQL(MySQL协议)方式直接访问MongoDB。
业务中特定类型敏感数据的识别	如我司大量病历、检查报告在系统中以特定格式URL传递，需要定制正则表达式规则进行识别。
数据分类分级清单耦合性过强	数据分类分级清单与安全措施耦合越强说明安全应用落地成熟，但需要注意数据分类分级结果变更对客体系统的影响，如：大数据系统、加密系统，需要提前做好流程和机制上的准备。
高敏感数据使用场景的元数据采集	高敏感数据据的使用、交换、存储需要重点监控和保护。需要尽早对其使用场景使用情况做数据采集，如：身份证展示和交换，需要采集系统、调用方法、API接口等信息。

信息来源：好大夫，西南证券整理

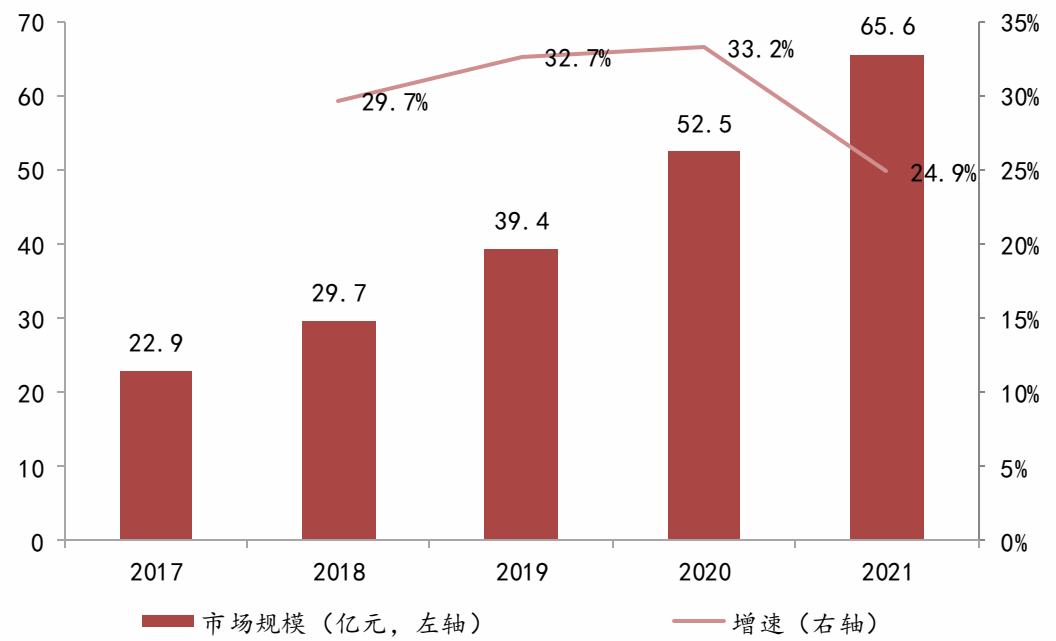
3.2 数据安全——市场规模

据海外市场研究机构VMR统计，**2019年全球数据安全市场规模约为173.8亿美元，预计到2027年全球数据安全市场规模将达到572.9亿美元（折合3835.51亿人民币），年复合增长率约为17.35%。**
随着我国经济的不断发展及各行业网络化建设的推进，我国数据安全行业市场规模不断扩大，**2021年市场规模达到65.56亿元，约占全球数据安全行业市场总规模的近20%，已经成为世界重要的数据安全市场；**根据信通院安全所信息安全部主任魏薇表示，**我国数据安全市场规模将在2023年预计达到97.5亿，届时数据安全在整体网络安全市场占比将达到12.1%。**同时我国数据安全行业市场规模保持了30%的年均复合增长率，高于全球市场规模21%的增速，因此我国数据安全市场已经成为全球数据安全行业重要的增量市场，且预计未来我国在全球数据安全行业中的比重会进一步增加。

2019-2027年全球数据安全市场规模



2007-2021年中国数据安全市场规模



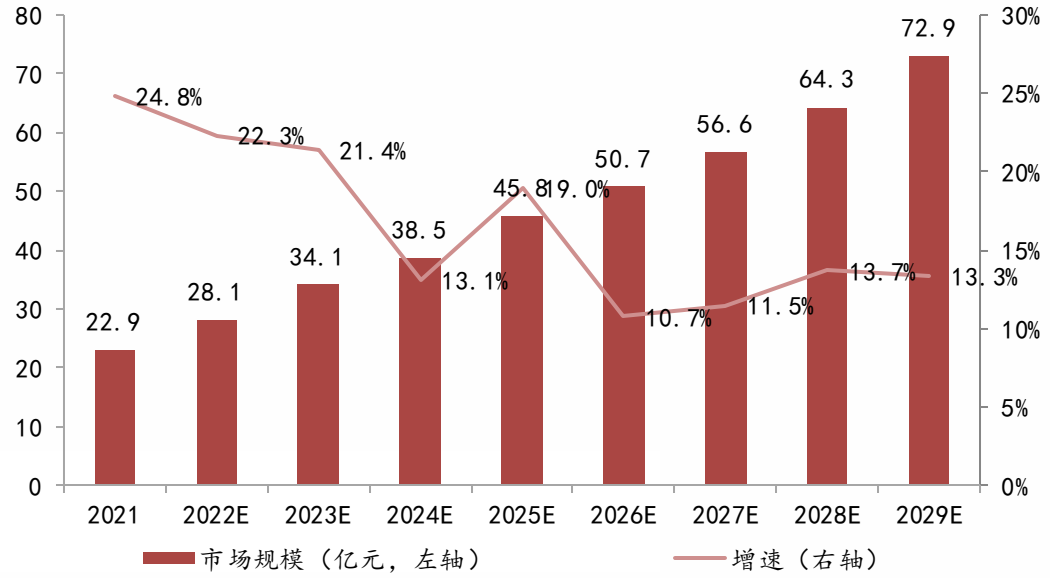
数据来源：观研天下，信通院，VMR，西南证券整理

3.2 数据安全——细分市场规模

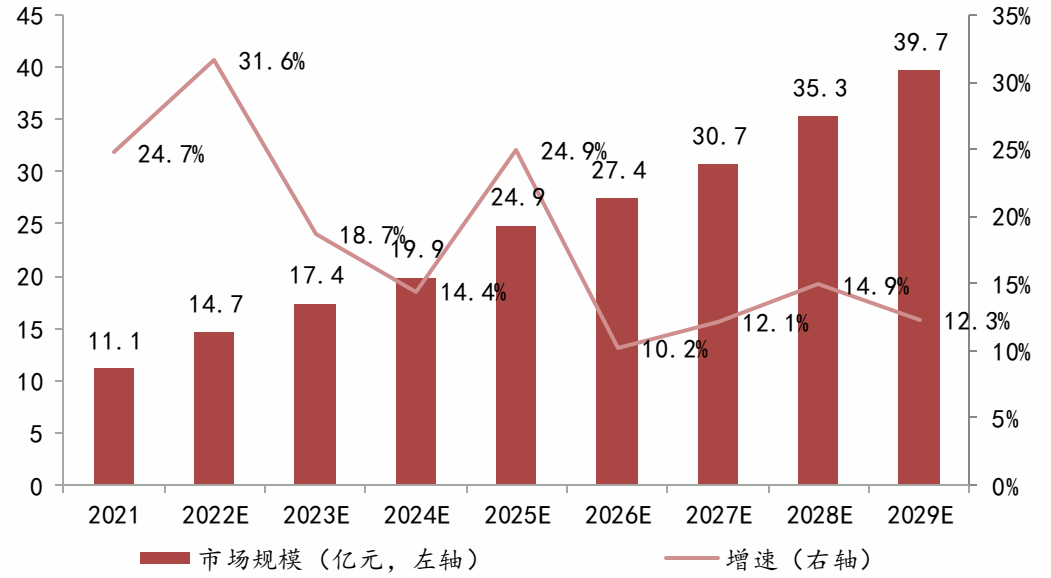
目前，数据安全正逐步成为关系到我国政府信息化以及数字政府建设工作能否顺利推进的关键因素，因此得到各级政府的高度重视。**近年来我国政府部门数据安全市场成为我国数据安全市场中占比最大的细分市场，2021年达到22.94亿元；预计2022年市场规模将达28.06亿元，同比增长22.3%。**

随着我国军工行业信息化建设不断推进，各企事业单位建立了自己的内部计算机网络及信息系统。军工行业信息化有着自身的特殊性，信息和数据泄密成为巨大威胁。根据国家保密局发布的《计算机信息系统保密管理暂行规定》和《BMB-17》系列分级保护要求，要求对涉密信息系统进行防护。**因此，目前军工部门数据安全市场成为我国数据安全市场中占比第二位的细分市场，2021年市场规模达到11.14亿元；预计2022年市场规模将达14.66亿元，同比增长31.6%。**

2021-2029年我国政府部门数据安全市场规模及预测



2021-2029年我国军工部门数据安全市场规模及预测



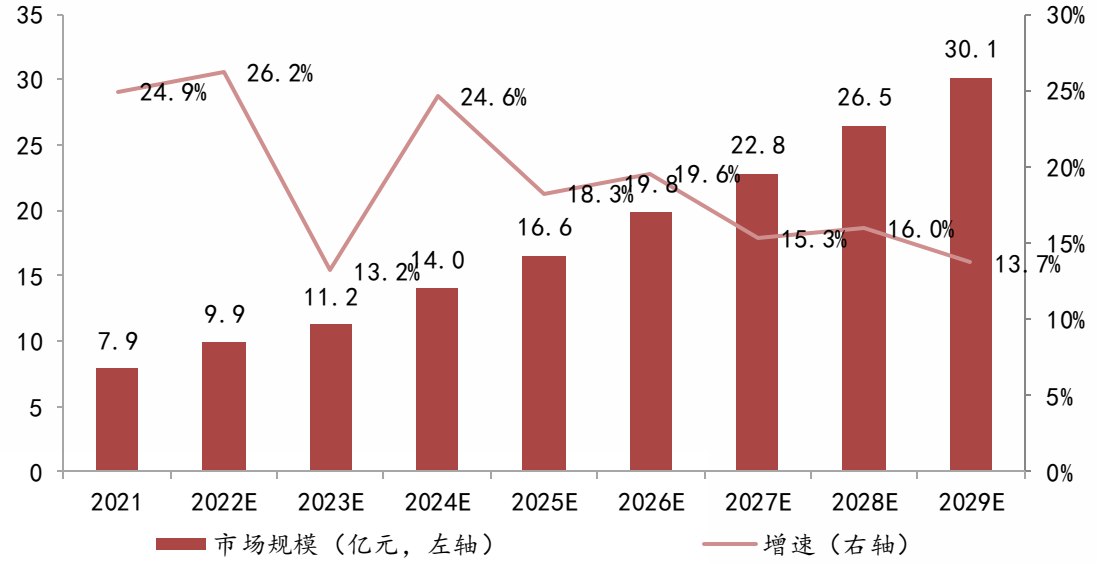
数据来源：观研天下，西南证券整理

3.2 数据安全——细分市场规模

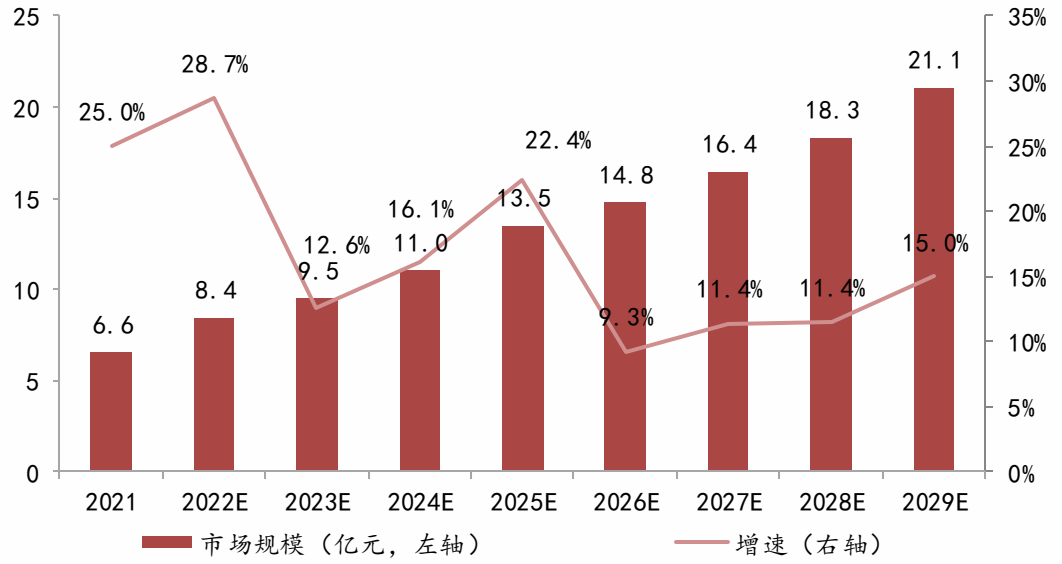
金融行业目前成为我国数据安全市场中第三大应用领域，2021年金融行业数据安全市场规模达到7.87亿元；预计2022年市场规模将达9.93亿元，同比增长26.2%。金融行业作为一个数据密集型、高安全标准和强监管的行业，在传统的以机密性、完整性、可用性为核心的数据安全领域已经建立了比较完善的技术体系。未来，随着《个人信息保护法》的推行，我国金融行业数据保护建设将以用户为中心、持续升级隐私和数据保护技术，通过建设全生命周期的安全保障平台，实现智能化、自动化数据安全保护运营。**2029年，我国金融行业安全市场规模预计将达到30.12亿元。**

目前我国电信行业同样成为数据安全行业市场中重要的细分市场，2021年其市场规模达到6.56亿元。随着我国电信行业数据安全标准体系的逐步建立，数据安全工作对促进数据应用规范化、提升数据活动安全性有着重要意义。我国电信行业数据安全市场规模将继续保持增长态势，**预计2022年市场规模将达8.44亿元，同比增长%；2029年其市场规模将达到21.05亿元。**

2021-2029年我国金融行业数据安全市场规模及预测



2021-2029年我国电信行业数据安全市场规模及预测



数据来源：观研天下，西南证券整理

3.2 数据安全——竞争格局

我国数据安全市场呈现出互联网巨头、专业数据安全服务商、传统网络安全企业三分天下的竞争格局。

- 互联网巨头：以**阿里巴巴、腾讯、百度**为代表的互联网公司借助其资本、人才及品牌优势布局数据安全市场，互联网巨头**通过投资并购的方式加深企业在数据安全市场的渗透，增加业务辐射范围。**
- 专业数据厂商：以**安华金和、奇安信、天融信**等企业为代表的专业数据安全服务商凭借其技术优势布局中国数据安全市场。专业数据安全服务商通过构筑技术壁垒，研发核心技术，实现单品向产线化扩张，加深产品在各应用领域的渗透率，提升自身竞争力。
- 传统网络安全厂商：以**启明星辰、360企业、卫士通、美亚柏科**等企业为代表的网络安全企业在资源方面优于其他行业参与者，例如卫士通、启明星辰在安全、管理和平台运营等业务领域拥有众多政府和军工客户资源，是传统网络安全企业中政企类业务占比最大的两家企业。

我国数据安全市场竞争格局

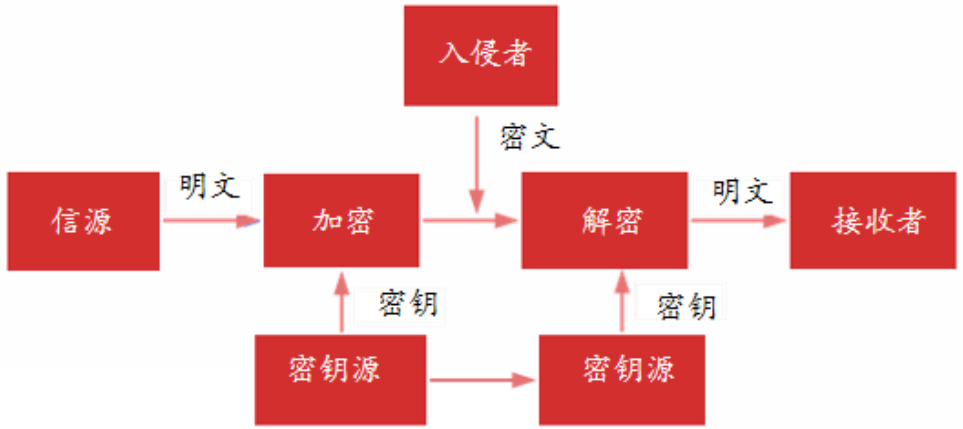
互联网巨头	专业数据厂商	传统安全厂商
Tencent 腾讯 Baidu 百度 Alibaba Group 阿里巴巴集团	DBSEC 安华金和 美创 MEICHUANG 天融信 TOPSEC 奇安信 EETRUST 时代亿信 Technology Company Limited	360 启明星辰 美亚柏科 MEIYA PICO Westone·卫士通 SANGFOR 深信服科技

信息来源：电子工程世界，头豹研究院，西南证券整理

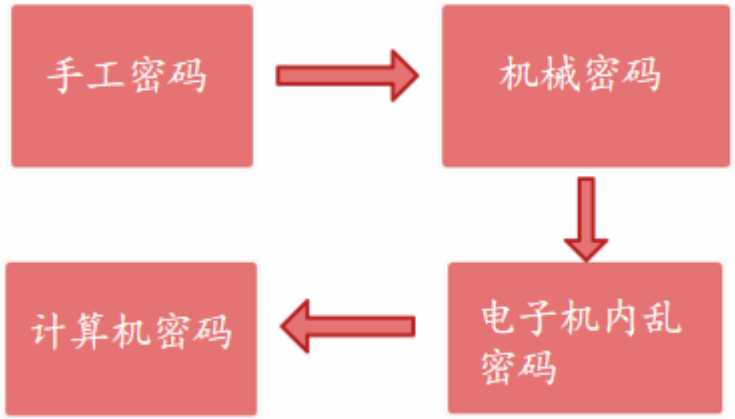
3.3 密码安全——定义

- **密码安全**：**在2021年之前称为“密码技术”，是数据加解密的基本过程。**密码安全就是对文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，使其只能在输入相应的密钥之才能显示出本来内容，通过这样的途径来达到保护数据不被非法窃取、阅读的目的。该过程的逆过程称为解密。
- **密码安全是保障网络与信息安全的核心技术和基础支撑**，通过加密保护和安全认证两大核心功能，可以完整实现防假冒、防泄密、防篡改、抗抵赖等安全需求，在网络空间中扮演着“信使”“卫士”和“基因”的重要角色。
- 密码安全按技术更迭可以分为**四个进程**：
  - **手工密码**：以手工方式完成加密，或以简单器具辅助操作的加密方式；
  - **机械密码**：以机械密码机或电动密码机来完成加解密；
  - **电子机内乱密码：**通过电子电路，以严格的程序进行逻辑运算；
  - **计算机密码：**以计算机密码软件进行算法加密解密，适用于计算机数据保护和网络通信等。

密码安全工作流程



密码安全技术发展



信息来源：数说安全，安全牛，西南证券整理

3.3 密码安全——法律法规

- **《中华人民共和国密码法》**：于2019年10月26日正式颁布，其颁布的主要目的其一是规范密码应用和管理，促进密码事业发展；其二是保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。
- 《中华人民共和国密码法》实施两年多来，我国密码工作的规范化、科学化、法治化水平得到显著提升，全社会密码安全和应用密码的意识普遍增强。值得关注的是，**近年来各地区各有关部门陆续出台了一系列促进商用密码产业发展的政策措施**，在资金补助、创新研发、人才引进、成果转化等方面给予实打实的支持，不断优化产业生态，商用密码正在迎来依法治理、供需互促、创新发展的新阶段。
- **《信息安全技术关键信息基础设施安全保护要求》：将于2023年5月1日正式实施。**
- 《关键信息基础设施安全保护条例》已于2021年9月1日正式实施，此次关保标准也是**第一项关键信息基础设施安全保护的国家标准**，有助于进一步提升国家关键信息基础设施安全保障能力和水平，推动我国网络强国战略实施、数字经济的健康良性发展。其中提到了**“商用密码应用安全性”评估，要求关键信息基础设施运营者每年至少进行一次安全检测评估**，评估内容包含网络安全等级保护制度落实情况、商用密码应用安全性评估情况、供应链安全保护情况、数据安全防护情况等。**“商用密码应用安全性”评估将加速商业密码应用的渗透。**

《中国人民共和国密码法》主要内容

目录	范围	主要内容
第一章	总则	规定了本法的立法目的、密码工作的基本原则、领导和管理体制，以及密码发展促进和保障措施。
第二章	核心密码、普通密码	规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施。
第三章	**商用密码**	**规定了商用密码标准化制度、检测认证制度、市场准入管理制度、使用要求、进出口管理制度、电子政务电子认证服务管理制度以及商用密码事中事后监管制度。**
第四章	法律责任	规定了违反本法相关规定应当承担的相应的法律后果。
第五章	附则	规定了国家密码管理部门的规章制定权，解放军和武警部队密码立法事宜以及本法的施行日期。

商业密码应用的渗透



信息来源：数说安全，安全牛，西南证券整理

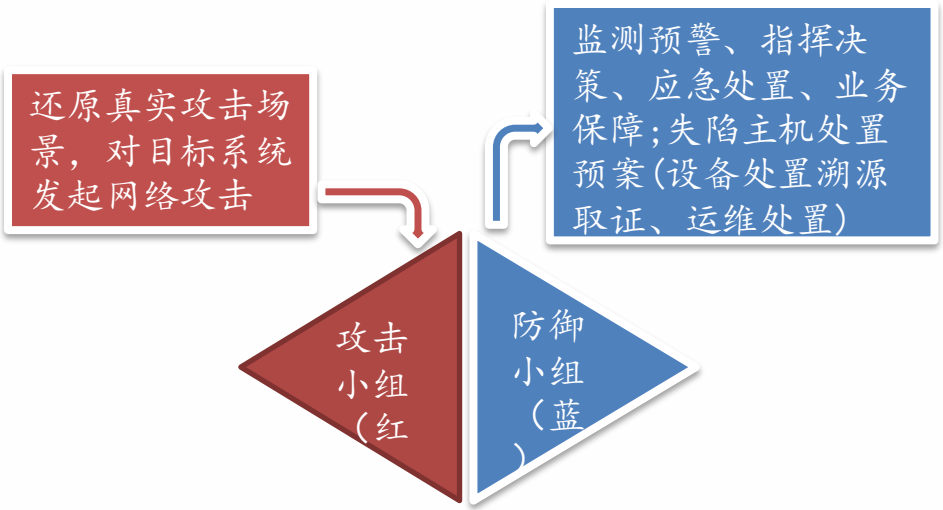
3.3 密码安全——等级测试

- **各个行业都要经过公安测试，均需经历“等保测评”、“护网行动”通报。**
- **“等保测评”：**“等保测评“是**信息安全等级保护测评**，是经公安部认证的具有资质的测评机构，依据国家信息安全等级保护规范规定，对信息系统安全等级保护状况进行检测评估的活动。**等保测评对于不同领域有不同的认定标准。**信息系统运营、使用单位应当选择符合国家要求的测评机构，依据《信息安全技术网络安全等级保护基本要求》等技术标准，定期对信息系统开展测评工作。
- **2019年5月13日，**国家市场监督管理总局、国家标准化管理委员会发布了3个网络安全领域的国家标准（2019年12月1日起实施）：《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）；《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）；《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019），**标志着我国进入等级保护2.0时代。**
- **“护网行动”：护网行动是一场网络安全攻防演练，是针对全国范围的真实网络目标为对象的实战攻防活动。**各大企事业单位、部属机关，大型企业(不限于互联网)，一般持续时间为三周。**在未来，护网行动将会进一步扩大，同样网络安全人才的缺口会进一步扩大。**

部分行业信息安全等级认定标准

金融行业	《信息安全技术金融信息服务安全规范》	《网上银行系统信息安全通用规范》	《金融行业信息系统信息安全等级保护实施指引》
	《金融行业信息系统信息安全等级保护测评指南》	《金融行业信息安全等级保护测评服务安全指引》	《云计算技术金融应用规范技术架构》
	《云计算技术金融应用规范安全技术要求》	《云计算技术金融应用规范容灾》	……
电力行业	《电力行业信息系统安全等级保护基本要求2012》	《电力行业信息系统安全等级保护基本要求2020》	《电力行业重要信息系统安全等级保护定级建议(电监会发)》
	《电力信息系统安全等级保护实施指南》	《电力信息系统安全检查规范》	《电力监控系统网络安全防护导则》
	《电力信息系统安全等级保护实施指南》	《电力监控系统网络安全评估指南》	……
政府	《信息安全技术政府门户网站系统安全技术指南》	《信息安全技术政府联网计算机终端安全管理基本要求》	《政府部门信息技术服务外包信息安全管理规范》
	《信息安全技术政府网站云计算服务安全指南》	……	

护网行动行动模型



信息来源：数说安全，安全牛，西南证券整理

3.3 密码安全——重要产品

密码安全公司及产品布局

公司名称	公司简介	产品布局
卫士通信息产业股份有限公司	成立于1998年，是中国电子科技集团有限公司（以下简称“中国电科”）旗下中国电子科技网络信息安全有限公司（以下简称“中国网安”）控股子公司。	**为党政、军队、大型央企等客户提供**专业的网络信息安全产品和服务，在加密认证类产品市场长期保持领先，在高安全信息系统集成市场占据重要地位，成功在业内树立起“信息安全国家队、密码产业主力军”的品牌形象，已发展成为国内有相当影响力的大型综合类安全企业。
北京数字认证股份有限公司	成立于2001年，是北京市国有资产经营控股有限公司控股的国有企业，2016年在深交所上市。	拥有16项专利、195余项软著，公司通过不断升级产品，**在行业推出了“信手书手写签名”、“信步云移动签名”、“易签盾生物识别签名”等产品，产生了“第一张电子保单”、“第一张电子彩票”、“第一张手写电子合同”、“第一张电子发票”、“第一张电子成绩单”**等多项创新产品。
格尔软件股份有限公司	成立于1998年3月，北京设营销和技术支持中心。公司下设北京格尔国信、上海格尔信息、上海格尔卫信及宁波格尔天屹等子公司。	**通过ISO9001质量体系认证，在做CMMI认证，通过CMMI3级，正向CMMI4级冲刺。承担了许多国家重点项目，**包括：中央办公厅RH项目、国家某部委BH项目、公安部等级保护项目、国家信息安全应用示范工程（S219）、国家863计划“数字证书应用综合管理”课题、信产部“3G无线通讯安全”课题、人民银行“IC卡密钥管理系统”项目等十六项。
北京炼石网络技术有限公司	成立于2015年，2020年获腾讯投资，2021年12月，入选北京市2021年度第七批“专精特新”中小企业名单。	**自主研发了CASB业务数据加密平台和高性能国密产品，**基于AOE面向切面加密技术打造“以密码技术为核心，访问控制、审计等多种安全技术互相融合”的实战化数据安全密码防护体系。
三未信安科技股份有限公司	成立于2008年8月，在上海、南京、广州、深圳、成都、重庆、武汉、西安、长沙等地设有子公司或分公司。	三未信安的**主要产品包括：密码芯片、密码板卡、密码整机和密码系统。**推出了国内首款安全三级密码板卡和首款安全三级密码整机，5次获得国家密码科技进步奖。
重庆沙海信息科技有限公司	成立于2009年，在北京、重庆设立了研发中心和运营机构。国家公安部认证的计算机信息安全产品销售许可单位。	**基于PKI体系，以自主的数项发明专利，**打造了智能化、体系化的数据全密文运行系列产品，形成了数据从采集、传输、存储、使用到销毁等全生命周期安全防护解决方案，塑造了防黑客攻击、防厂商泄露、防内部威胁的数据安全三防体系。
江南科友科技股份有限公司	历经20年发展，已形成了以京、沪、穗三地营销/服务中心为骨架，覆盖全国主要省份的办事机构。	公司**自主研发的“运维安全审计系统”、“密码服务系统”、“支付服务密码机”、“网络加密机”**等多种产品通过国家商用密码管理局技术认证，在金融信息化建设、电子支付安全服务、电子政务和社会信息化安全等领域广泛应用。
深圳奥联信息安全技术有限公司	成立于2002年，与西安电子科技大学合作成立“西电密码研究中心”，在北京、长沙、西安、贵阳等区域设立分子公司。	在IBC标识密码技术研究和应用上处于国际领先水平，**自主或参与设计的多个标识密码算法已被ISO、IEEE、3GPP和IETF等国际标准组织采纳为标准算法；**目前已主导或参与了国际标准7项、国家标准8项、行业标准8项的制定工作。
深圳市东进技术股份有限公司	成立于1993年，总部位于深圳。	以创新扎根于通信行业，**开创了一系列CTI行业第一，自主研发出国内第一块语音卡，推出国内首次采用DSP技术的计算机语音通讯产品，装机端口数稳居同行业第一位。**

信息来源：数说安全，安全牛，西南证券整理

3.4 身份与访问安全——定义

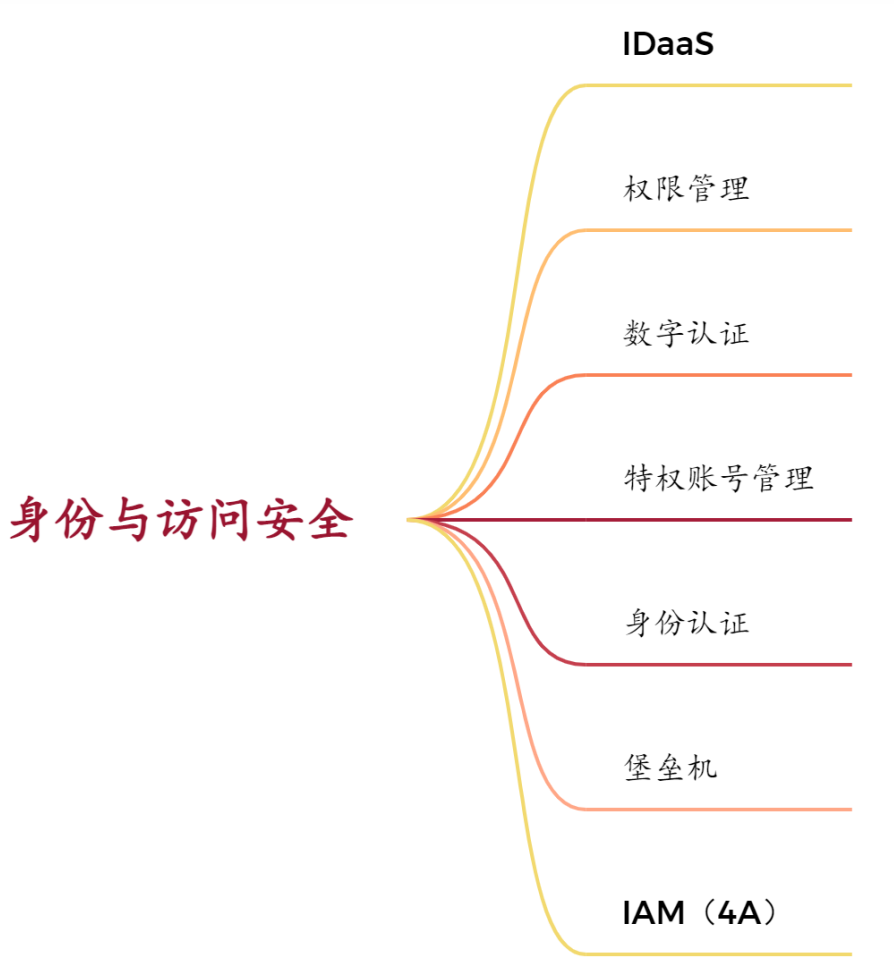
身份与访问管理（IAM）是让合适的自然人在恰当的时间通过统一的方式访问授权的信息资产，提供集中式的数字身份管理、认证、授权、审计的模式和平台。IAM是一种安全规程，主要系统和流程包括“IT管理员为每个实体分配单一数字身份”、“在登录时对其进行身份验证”、“授权访问指定资源”以及“在其整个生命周期中监控和管理这些身份的系统和流程”。

用户身份验证是IAM系统的关键任务之一，其类型主要包括三类：单点登录、多重身份验证、基于风险的身份验证。

- 单点登录（SSO）：单点登录(SSO)解决方案可提高生产力并减少用户的阻力。通过一次输入一组登录凭据（用户名和密码)，个人可以访问多个应用程序，并在它们之间无缝切换。
- 多重身份验证（MFA）：通过要求用户提供用户名之外，还要求用户另外两种或更多种识别凭据来获得对应用程序的访问权限，从而增加了另一层保护。例如，您可能会被要求输入密码和通过电子邮件或短信发送的临时代码。
- 基于风险的身份验证：也称为自适应身份验证，这是一种基于风险的身份验证解决方案，仅在检测到存在更高风险时才提示用户进行MFA。例如，当用户的位置与基于IP地址的预期不同或检测到恶意软件时，可能会出现这种情况。

根据安全牛发布的《中国网络安全行业全景图（第九版）》，**身份与访问安全涉及IDaaS、权限管理、数字认证、特权账号管理、身份认证、堡垒机、IAM（4A）等7大细分领域。**

身份与访问安全细分领域



信息来源：百度百科，IBM，安全牛，西南证券整理

3.4 身份与访问安全——重要产品

身份与访问安全领域重要产品

产品名称	简介	领域
阿里云应用身份服务(IDaaS)	应用身份服务IDaaS是阿里云原生企业身份管理服务，旗下EIAM（EnterpriseIAM）用于保护企业内部身份、CIAM（CustomerIAM）提供面向外部会员的身份管理、安全认证集成了多种无密码认证方式，加强登录安全。	IDaaS
吉大正元权限管理系统	包括： PMS管理终端：基于Web浏览器的管理模式，支持当前主流的浏览器。 权限管理服务：负责梳理各个应用系统的人员、机构、属性、角色信息，并将以上信息在权限管理模块内进行注册，最后完成人到角色（或权限）、机构到角色、属性到角色的绑定关系维护。 属性证书签发服务：应用系统会信任属性权威源签发的属性证书，并以属性证书所签发的内容进行系统内部的访问控制操作。属性证书签发模块负责建立属性权威源，并负责将“权限管理模块”中人到角色、群体到角色的映射关系签发成属性证书，并将已经签发成功的属性证书返回给“权限管理模块”。	权限管理
数字认证·数字认证服务	该服务是数字认证公司作为独立、公正、权威的CA机构向各类用户发放数字证书的服务平台，能够进行数字证书的申请、审核、签发、下载、更新、查询、吊销等全生命周期管理。所发放的数字证书，存储了证书所有者信息、公开密钥和颁发机构等，用以标识个人、单位、设备等在网络中的数字身份，确保网上传递信息的安全性、完整性。	数字认证
奇安信特权账号管理系统（PAM）	特权账号管理系统（PAM），是以数据的重要访问入口——账号口令安全为维度的数据安全产品，能够主动发现各类基础设施资源的账号分布、识别账号风险（包括弱口令、僵尸账号、幽灵账号、长期未改密账号，账号违规提权等）、管理账号使用，实现对各类基础设施资源账号的全生命周期管理，帮助客户提升账号安全的主动防御能力，降低因账号口令泄漏或被非法利用而造成的数据外泄风险。	特权账号管理
深信服SSLVPN	SSLVPN的突出优势在于Web安全和移动接入，它可以提供远程的安全接入，而无需安装或设定客户端软件。SSL在Web的易用性和安全性方面架起了一座桥梁。目前，对SSLVPN公认的三大好处是：首先是它的简单性，它不需要复杂配置，可以立即安装、立即生效；第二个好处是不需要安装客户端，直接利用浏览器中内嵌的SSL协议就行；第三个好处是兼容性好，可以适用于任何的终端及操作系统。	身份认证
天融信运维安全审计系统	天融信运维安全审计系统TopSAG是基于自主知识产权NGTOS安全操作系统平台和多年网络安全防护经验积累研发而成，系统以4A管理理念为基础、安全代理为核心，在运维管理领域持续创新，为客户提供事前预防、事中监控、事后审计的全方位运维安全解决方案，适用于政府、金融、能源、电信、交通、军队、教育等行业。可实现账号管理、身份认证、集中授权等功能。	堡垒机
吉大正元IAM系统	该系统通过建立一套统一的身份认证管理平台，确保可信的主体（人、设备、应用）在恰当的时间和地点（国内、外），通过可信的访问链路，以多种认证方式，安全合规的访问已授权的客体（应用后台、应用功能、数据或服务接口）。	IAM（4M）

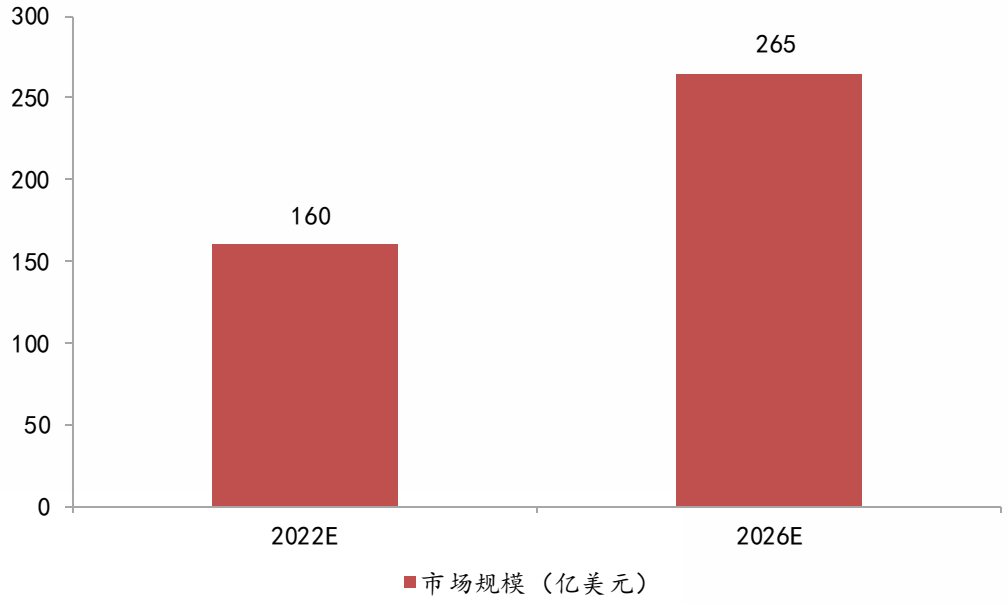
信息来源：阿里云、吉大正元、数字认证、奇安信、深信服、天融信公司官网，西南证券整理

3.4 身份与访问安全——市场规模

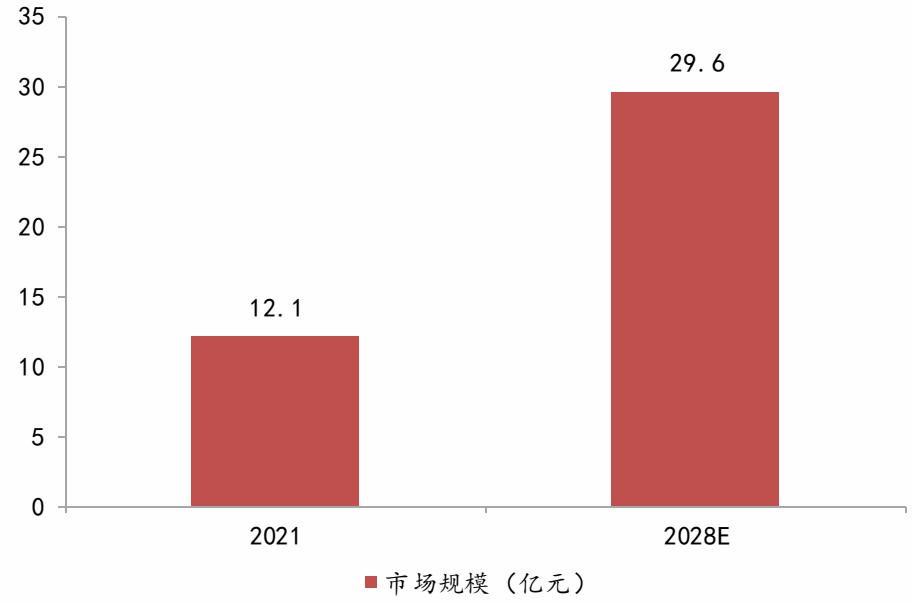
Gartner数据显示，自2017年以来，身份和访问管理市场全球安全支出呈现出逐年增长的趋势。2017年身份和访问管理市场全球安全支出为88.2亿美元，2018年支出为97.7亿美元。2019年身份和访问管理市场全球安全支出突破100亿美元，达到105.8亿美元。**根据Juniper数据，2022年全球IAM支出达到160亿美元，2026年将达到265亿美元，四年复合增速可达13.4%。**

网络身份认证是信息安全防护第一关口，具备重要地位。下游行业网络安全建设推动身份认证信息安全市场持续增长。身份认让信息安全行业的下游行业目前以银行业为主，现已逐步发展到证券、工商税务、电子政务、电子商务、企事业OA/VPN系统、弟三方支付、移动支付、云计算、IC卡等众多领域。随着网上银行的推广和发展以及其他信息系统安全性要求的提高，身份认证市场将面临市场增长需求。**2021年，中国身份和访问管理(IAM)软件市场规模达到了12.11亿元，预计2028年将达到29.57亿元，7年CAGR为12.66%。**

2022-2026年全球身份与访问管理市场规模



2021-2028年中国身份与访问管理市场规模

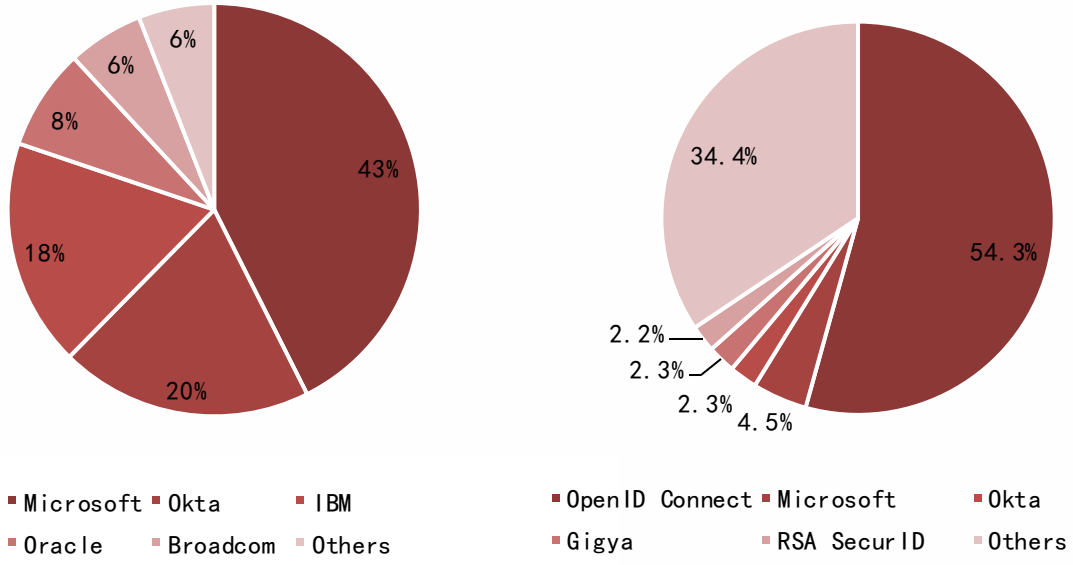


数据来源：Gartner，Juniper，GlobalInfoResearch，西南证券整理

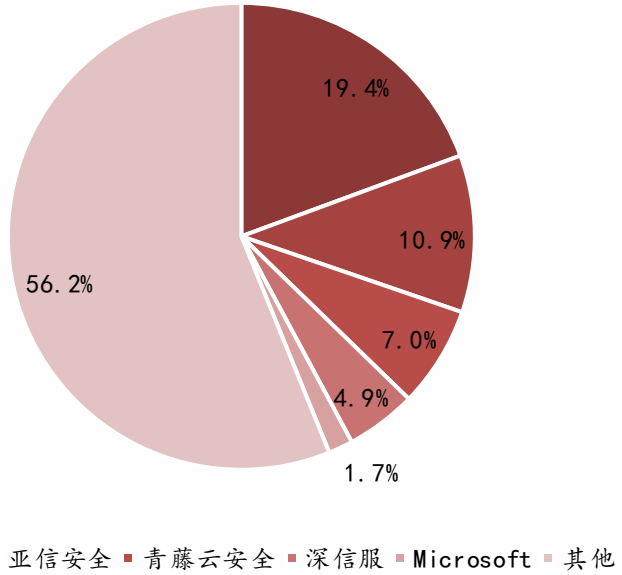
3.4 身份与访问安全——竞争格局

根据Statista，2021年占IAM全球市场份额最大的是OpenIDConnect（OIDC），其是一个基于OAuth2.0规范的可互操作的身份验证标准协议，并不作为商业应用，使用它不需要任何费用、任何注册或者许可证，**紧跟其后的IAM厂商有Microsoft、Okta以及Gigya，分别占比4.5%、2.3%、2.3%。**剔除了OIDC的影响后，**2019年IAM市场份额占比最大的为Microsoft（43%），其次是Okta占比20%，已经超过了大型龙头企业IBM以及Oracle，说明了客户对Okta能力的认可和信赖。**
2021年中国身份和数字信任软件市场份额**中亚信安全占比最多，达11.3%。**其次分别为**数字认证、吉大正元、格尔认证、信安世纪，**占比分别为7.7%、7.1%、6.4%及5.4%。

2019年和2021年全球身份与访问管理市场竞争格局



2021年中国身份与数字信任软件市场竞争格局



数据来源：Statista，IDC，西南证券整理

3.5 零信任——定义

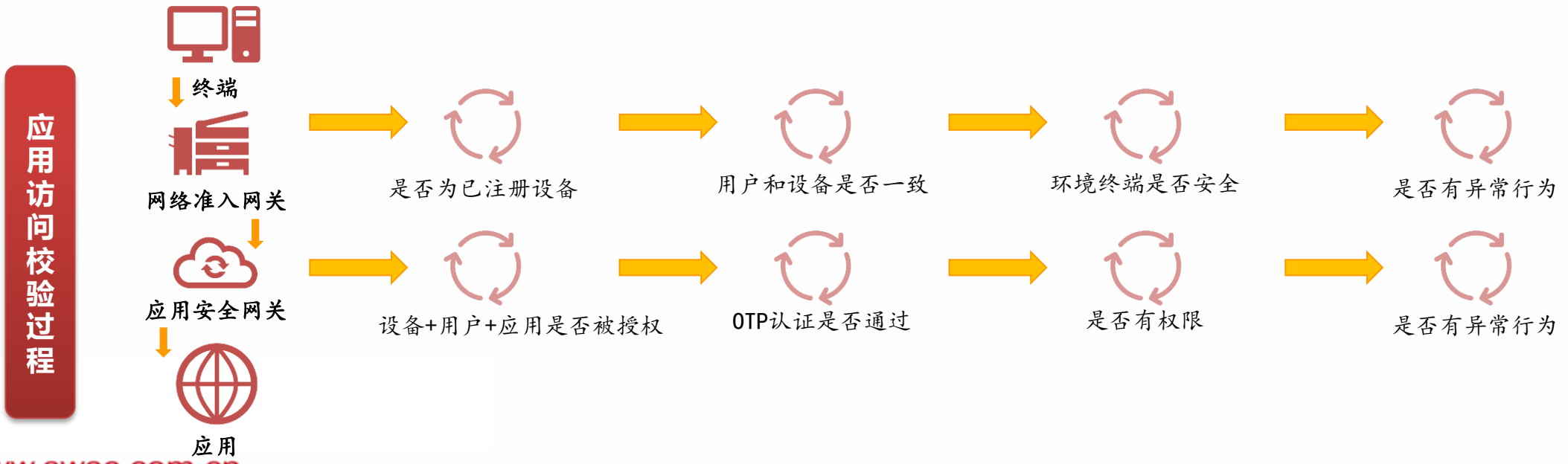
➢ 为什么要实施零信任架构

主动防护有以下难点：

1. IT基础治理建设不完善：资产、账号、系统数量不明；
2. 供给面大量暴露：防火墙规则形同虚设，每个部门业务平台隔离，NAT对外暴露服务。建立内网可以打通各业务部门网络、减少NAT对外暴露服务。

基于对GoogleBeyondcrop架构分析，零信任架构有以下特点：

1. 不再重点区分内外网，哪个只是其中的一个结果；
2. 建立信任链条是核心，以做到动态持续的安全校验，缩小攻击面。网络准入网关建立了“用户+设备”的第一步信任链；应用安全权限建立了“设备+用户+应用信任链”



信息来源：完美世界，西南证券整理

3.5 零信任——架构构成

➢ 零信任架构

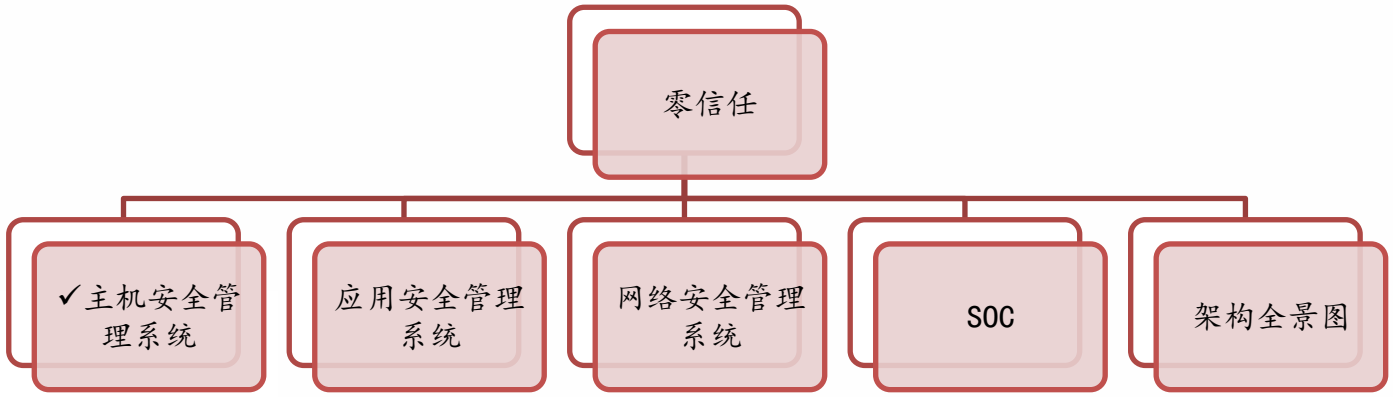
零信任并不是全新的技术，而是基于传统安全技术升级上来的解决或是整合方案，它**可以拆解为对以下几个问题的解决方案：**

- ✓ **用户与设备的认证管理问题**：主机安全管理系统
- ✓ **用户与应用的认证管理问题**：应用安全管理系统
- ✓ **用户设备的网络准入管理问题**：网络安全管理系统
- ✓ **动态分析检测的问题：**SOC
- ✓ **拼装问题**：架构全景图。

零信任现在充分应用于以下场景：

- ✓ **梳理资产变化**：建立“人->资产->资产属性->事件”多层结构关系，进而提高事故发生之后的问责效率；
- ✓ **无密码化**：零信任解决静态密码的弊端，传统架构下只要拿到管理员的密码，整个网络便岌岌可危。
- ✓ **远程办公**：做好用户的唯一化，用户和设备的关系映射，用户的权限分配是实现企业零信任的基础。

零信任架构拆解



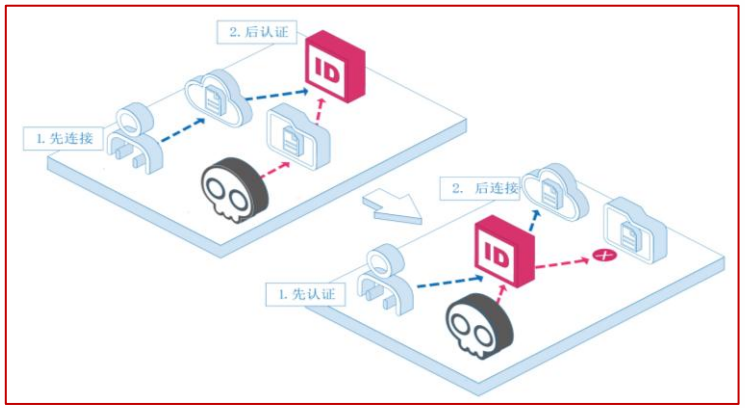
信息来源：完美世界，西南证券整理

3.5 零信任——特点

➢ 零信任架构的优势

1. **安全可靠性更高**：基于链条式信任关系，中间环节发生任何异常变化，都更容易被发现、被检测，防护相应速度快，因此安全可靠性更高；
2. **攻击难度大**：随着信任链条维度增多，黑客攻击成本提高，入侵的难度加大；由于用户的信任是通过生物校验和多因素认证，对设备的信任是通过主机准人关系，基线状态，运行状态判断等多维度验证建立，攻击难度加大；
3. **持续校验，从不信任**：每一次对资源的请求，都是一次重新校验的过程，安全的状态是动态，因此检测也是动态持续发生，这样如果产生了异常，可以迅速感知并阻断；

“从不信任，始终验证”原则



➢ 零信任架构的缺点

1. **单点故障导致业务中断风险**：因为对资源的控制都集中在网关上，一旦单点故障会导致整个业务中断；
2. **集中化权限风险**：零信任架构把很多风险收敛集中起来，但并非集中化风险就不存在了，比如集中化管理中，如果管理失控了会带更大风险；
3. **复杂化风险**：因为整个架构涉及多个组件，足够复杂，出现业务异常后容易出现问题不能及时发现和处理的情况；
4. **凭证风险**：为了平衡用户体验，一般零信任架构都会内置SSO功能，但该功能对于身份的凭证安全、或是注册设备的凭证安全问题、这些凭证的风险都可能会破坏信任体系；
5. **项目建设周期过长风险**：零信任架构建设周期比一般架构体系要来的长，这样可能会出现项目未完工，人已经走了的情况，后续接手的人是否还认可这个理念，是否要会从头来过等一系列投资风险。

信息来源：完美世界，西南证券整理

目 录

1 网络安全客户采购驱动因素

2 网络安全行业发展趋势

3 网络安全核心细分领域

3.1 防火墙
3.2 数据安全
3.3 密码安全
3.4 身份与访问安全
3.5 零信任

4 网络安全行业国内外对比

4.1 产业生态
4.2 竞争格局
4.3 人员构成

5 网络安全厂商未来核心竞争力

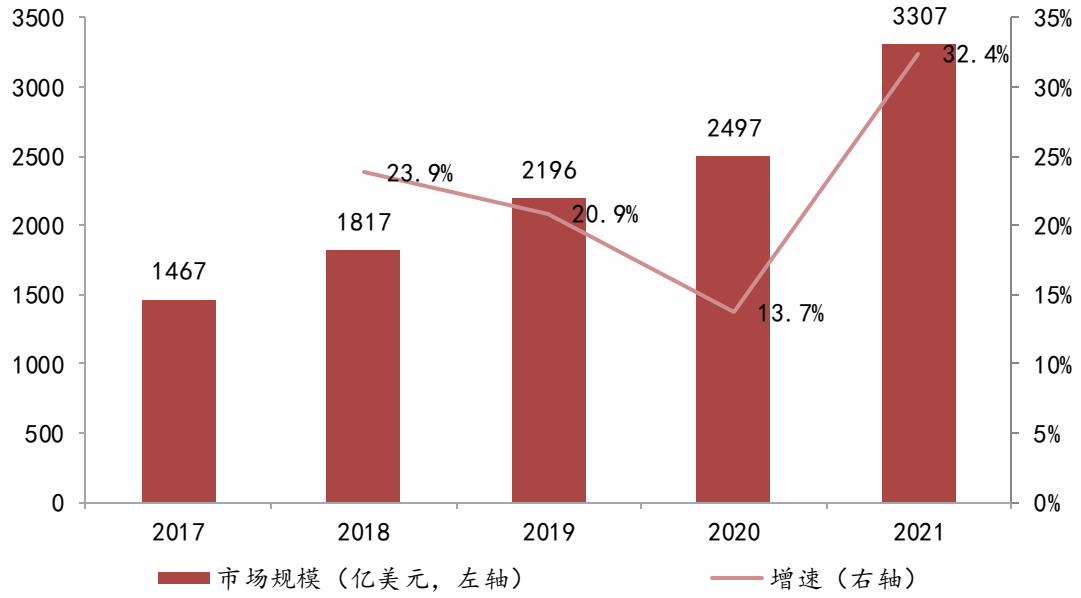
4 网络安全国内外对比—产业生态

➢ 云环境基础设施

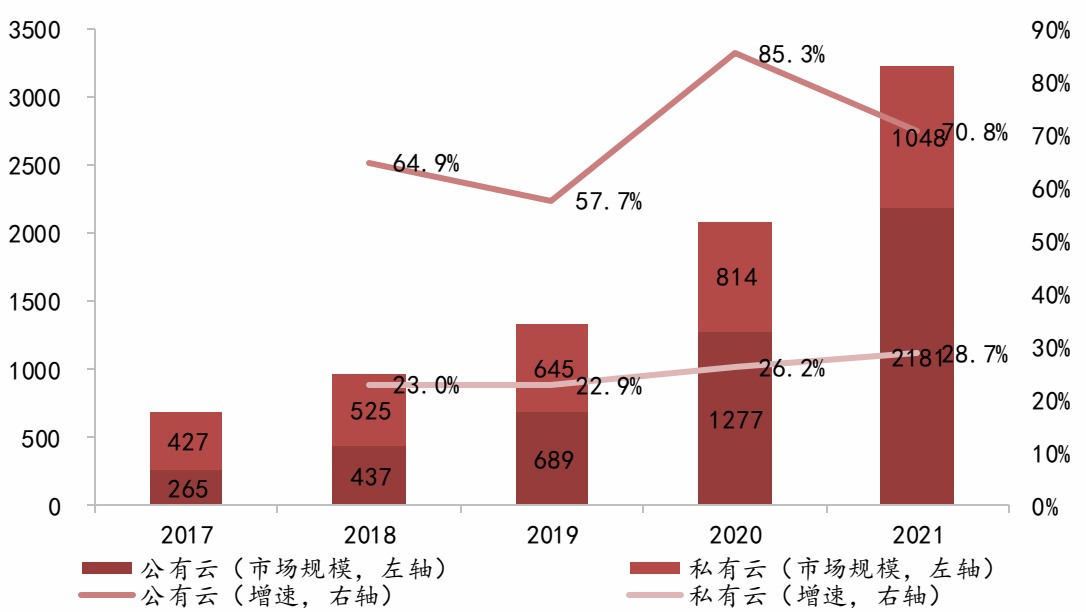
公有云、私有云和混合云共同组成现有云环境。

- **海外云环境以公有云为主，**2021年全球公有云市场规模达3307亿美元，同比增长32.4%；
- **我国公有云、私有云并存，私有云占比约1/3。**2021年我国云计算市场规模达3229亿元，同比增长54.4%。其中，公有云市场方兴未艾，快速增长，2021年市场规模达2181亿元，同比增长70.8%；私有云市场首次突破千亿大关，2021年市场规模达1048亿元，同比增长28.7%。此前，中国云环境一直保持着私有云、公有云“二分天下”的格局，2021年公有云市场占比首次大幅超越私有云市场占比，形成公有云、私有云“2：1”的市场组成。

2017-2021年全球公有云市场规模



2017-2021年中国云环境构成（亿元）



数据来源：Gartner，中国信通院，西南证券整理

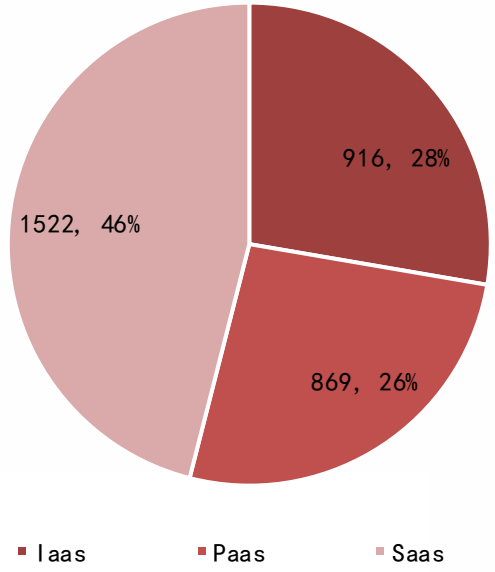
4 网络安全国内外对比—产业生态

➢ 云环境基础设施

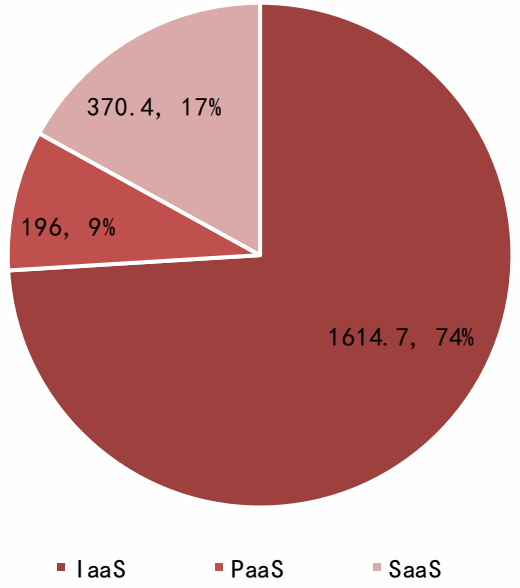
公有云有IaaS、PaaS、SaaS三大细分领域。

- **海外公有云市场以SaaS为主，**2021年全球公有云市场规模达3307亿美元，其中**SaaS市场规模达1522亿美元，占比46.0%；**IaaS市场规模916亿美元，占比28%；PaaS市场规模869亿美元，占比26%。
- **我国公有云市场以IaaS为主。**2021年我国公有云市场规模达2181亿元，其中**IaaS市场规模达1614.7亿元，占比74.0%；**PaaS市场规模196亿元，占比9%，SaaS市场规模370.4亿元，占比17%。

2021年全球公有云市场构成（亿美元）



2021年中国公有云市场构成（亿元）



数据来源：Gartner，中国信通院，西南证券整理

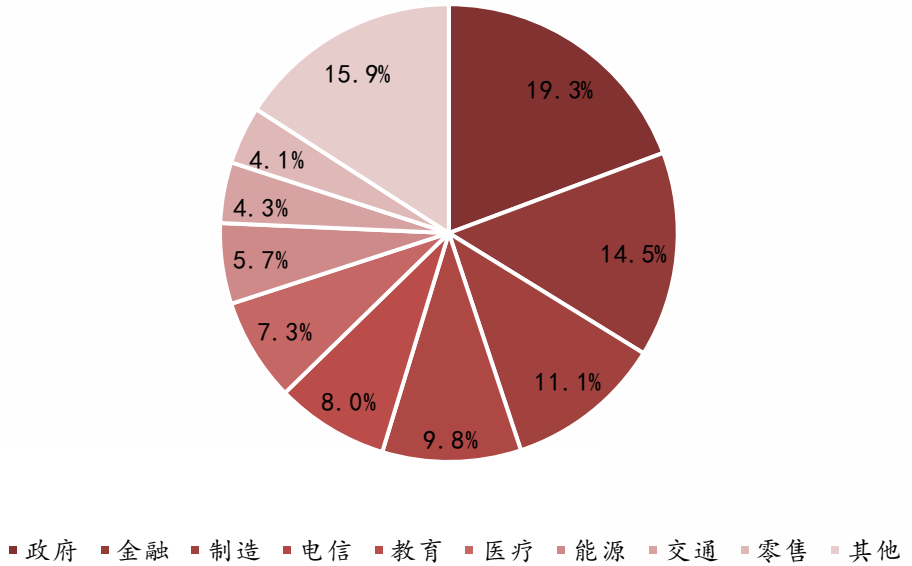
4 网络安全国内外对比—产业生态

➢ 客户构成

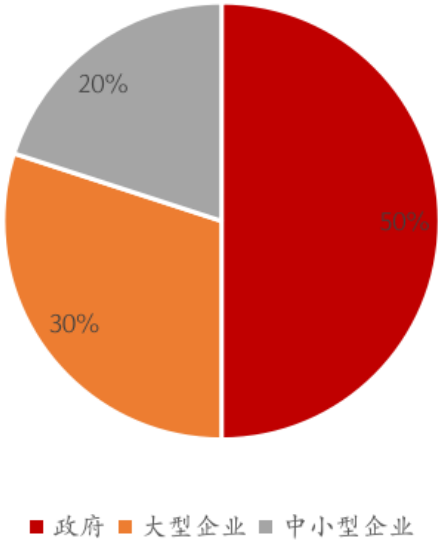
由于云环境基础建设现状不同，国内外网络安全客户构成大相径庭。

- **海外公有云基础建设完善，SaaS化程度、云渗透率高，客户以企业为主，根据Frost&Sullivan数据，全球网络安全市场中政府客户仅占比19.3%。**
- **我国网络安全市场客户所属行业分布与我国云环境建设现状相关性强。**我国云计算发展落后于海外，导致目前网络安全公有云渗透不高；且政府客户选择私有云为主，云环境中私有云占比高，因此，我国**网络安全行业中，政府客户数量占比达到50%，**其次大型企业包括医疗卫生、教育、能源化工等行业客户数量占比达到30%，小型企业客户数量占比达到20%。

全球网络安全行业市场应用领域占比



网络安全公司客户占比



数据来源：Frost&Sullivan，中国网络安全产业联盟，西南证券整理

4 网络安全国内外对比—产业生态

➢ 法律法规

十年前，**海外的网络网络安全主要产品已出现云安全、XDR等产品，且以SaaS产品为主，我国在2020年前后才逐渐有云安全产品。同时海外对于网安的法律体系建设也早于我国。**就美国而言，网安在本世纪初已被提升至国家战略地位，我国在近十年才进入以关键信息保护基础建设的新阶段。

中美网络安全产业形态、产业法规对比

时间轴	1980S	1990S	2000S	2010S	2020至今
网络防御主要产品	早期反病毒软件出现	安全产品放量	防护技术提升	云技术普及，网络安全产品云化	新技术频现
美国	防病毒软件	防火墙、VPN等迅速放量	UTM、下一代防火墙诞生	云安全、XDR等	零信任、机器学习产品
中国		杀毒软件瑞星、江民和金山“三足鼎立”	FW、入侵检测/防御等安全硬件诞生	政企安全市场格局分散，群雄割据	基于PaaS、SaaS的云安全产品
网络防御相关政策					
美国	拉开网络安全制度建设序幕 1977年《联邦计算机系统保护法》 1979年《国家安全通信政策》 1987年《计算机安全法》 1999年《网络电子安全案等》等		网安上升至国家战略 2000年《保护美国的网络安全：国家信息系统保护计划》 2003年《确保网络安全国家战略》 2004年《保护网络空间国家战略》 2008年《国家网络安全倡议(CNCI)》 将网络安全扩展至重要基础设施领域等	完善网络安全立法 2014年《国家网络安全保护法》 2015年《网络安全信息共享法》 2015年《网络安全法》明确国土安全部在网安领域的主责地位 2016年《国家网络安全应急预案》 2018年《网络安全战略》 2022年《美国网络安全增强法(2022)》关键基础设施安全的战略地位全面与国家安全挂钩	
中国		网安“宣传启蒙” 1994年《中华人民共和国计算机信息系统安全保护条例》 1997年《计算机信息网络国际联网安全保护管理办法》	网安“有法可依” 2004年《电子签名法》 2006年《信息网络传播权保护条例》 2007年《信息安全等级保护管理办法》和2008年《信息安全等级保护基本要求》成为了我国非涉密信息系统网络安全建设的重要标准	进入关键信息保护基础建设新阶段 2016年《网络安全法》 2019年等保2.0 2020年十二部门联合发布《网络安全审查办法》 2021年《数据安全法》 2021年《关键信息基础设施安全保护条例》 我国网络安全保护进入了以关键信息基础设施安全保护为重点的新阶段	

信息来源：公安部，人大，中央政府，美国总务署官网，美国电子隐私信息中心EPIC，微信公众号“奇点安全”，西南证券整理

4 网络安全国内外对比—产业生态

➢ 产品形态

由于海外网安领域相关法律建设完善、产品标准化程度高，并且生态配套完全，聚焦单一产品的公司也能成为巨头。如网络安全领域的paloalto，终端安全领域的Sophos、Trend，身份安全领域的OKTA等。

由于我国相关法律建设进程较缓，**产品标准化仍有努力空间**，单一上市公司产品布局广泛而全面，但没有横向连接形成完整的产业生态，所以市场以项目制公司为主，主要提供定制化产品，初创公司难以突出重围。同时，**我国的安全产品形态落后，目前Saas化仍然不足**，12月9日，中国第一个公有云SaaS终端安全产品，亚信安全天穹（ImmunityOne）才正式上线AWSMarketPlace。下游客户采购网络安全产品大多作为单一的传统服务器使用。

美国网络安全主要参与者

网络安全：paloalto、FORTINET、zscaler、Checkpoint、CLOUDFLARE、cisco、Barracuda、JUNIPER

终端安全：CROWDSTRIKE、SentinelOne、SOPHOS、cybereason、TREND MICRO、Microsoft、BROADCOM、McAfee

身份安全：okta、PingIdentity、SailPoint、BeyondTrust、BROADCOM、IBM、ORACLE

网络安全：exabeam、securonix、CORTEX、DARKTRACE、LogRhythm、MICRO FOCUS、splunk>、IBM、RAPID7、humio

数据保护和隐私：VARONIS、Collibra、Chainalysis、druva、BigID Know Your Data、OneTrust

IOT/OT安全：CLAROTY、NOZOMI NETWORKS、ARMIS、SHIFT5、DRAGOS

安全服务：pwc、accenture、MANDIANT、IBM、ARCTIC WOLF、ESENTIRE

云安全：WIZ、LACEWORK、aqua、sonrai、illumio、orca security、SentinelOne、paloalto、CROWDSTRIKE

应用安全：snyk、SYNOPSYS 新思、perimeter x、Contrast、WhiteSource、Akamai、imperva、VERACODE、Checkmarx、CEQUENCE

腾讯云安全产品体系全景图



信息来源：Techsoho，腾讯云，西南证券整理

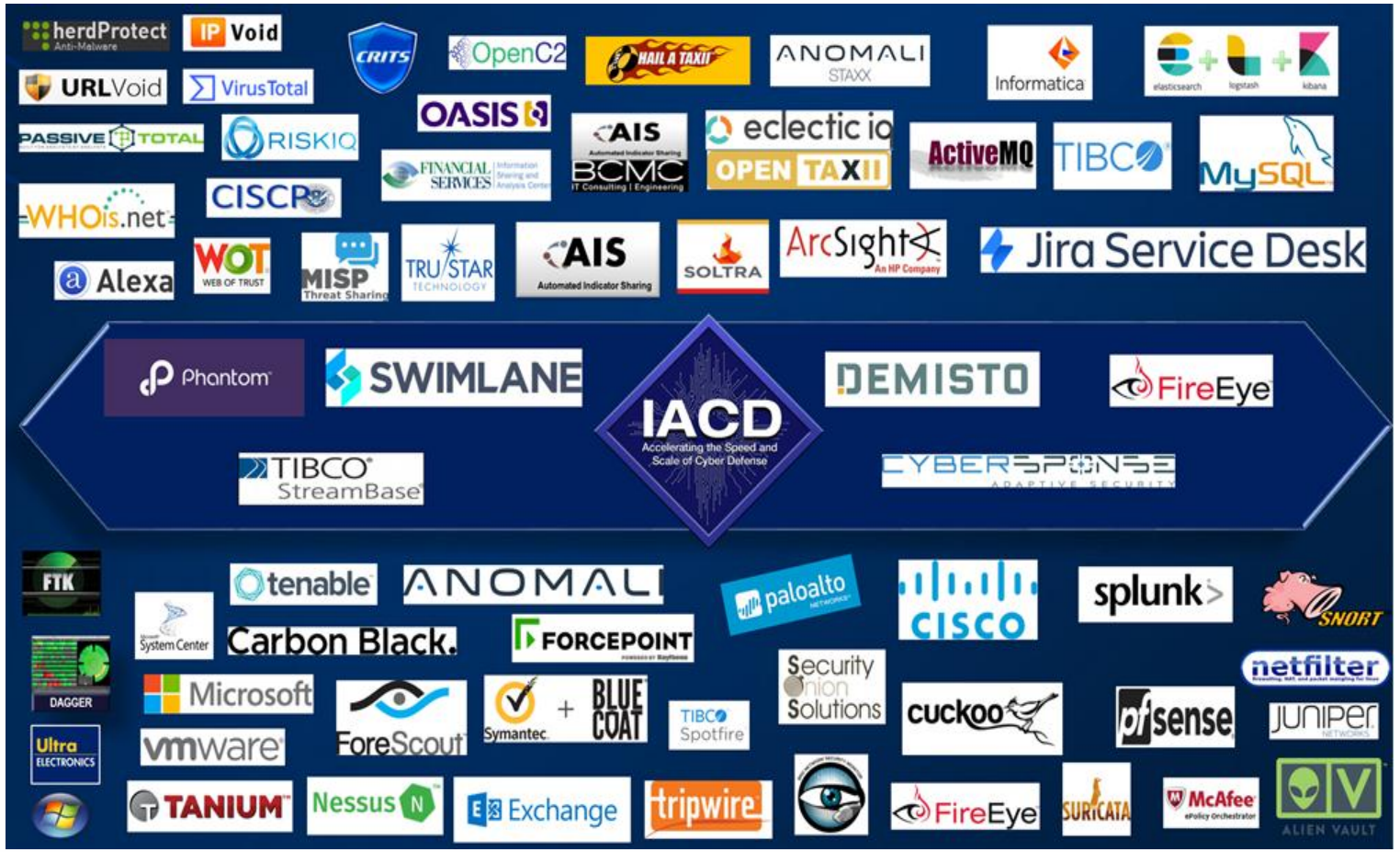
4 网络安全国内外对比—产业生态

➢ 新创公司处境

国外网安公司专注于一个小领域也能迅速崛起，主要有两点原因：

- **商业环境规范。**海外之所以有公司做起来，是因为商业环境比较规范，接口比较规范通用。国内情况不太一样，各家都有一套，专做身份认证就比较难做起来。**美国国土安全部（DHS）、国家安全局（NSA）和约翰•霍普金斯大学应用物理实验室（JHU/APL）联合发起的IACD，十分看重生态构建。目前IACD已集成了众多主流的安全厂商、机构、系统、产品和规范。**
- **技术投入较大。**技术研发需要时间和资金，每一种认证方式的细节做到非常完美、安全性做到非常高，需要比较大的投入。专业厂商在细节、安全性和兼容性等方面皆表现优异。同时，专业厂商容易展现规模效应和先发优势，他们会把深入渗透细分领域，得以体现它的竞争力和规模效应。

美国IACD产品集成生态



信息来源：腾讯云开发者社区，西南证券整理

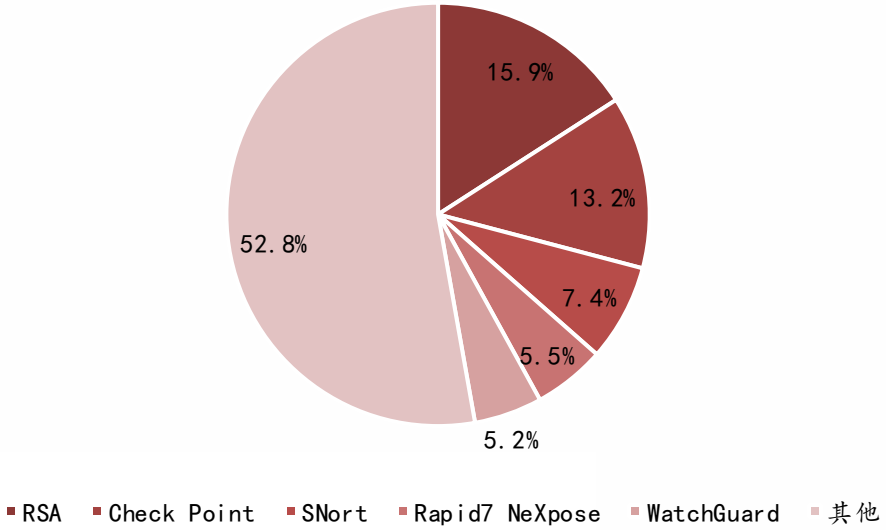
4 网络安全国内外对比—竞争格局

➢ 竞争格局

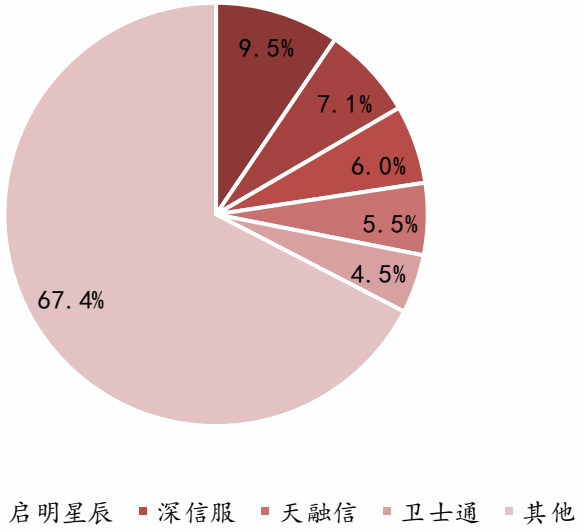
国外网络安全业务主要由网络安全软件厂商参与，依据Datanyze发布数据，截至2021年8月，全球网络安全软件细分领域，以美国老牌网安公司RSA和以色列网安公司CheckPoint市占率排名前二。其中，RSA在全球网络安全软件领域市占率为15.9%，CheckPoint为13.2%，其他企业市占率均在10%以下。

我国网络安全市场呈现低集中寡占性格局。现阶段，我国各网络安全厂商主要向市场提供诸如安全设计、安全评估、安全运维和安全技术研发等方面的安全服务，该细分**市场参与主体众多，模式尚不统一，竞争激烈，市场集中度低。**2020年，奇安信、启明星辰、深信服等三家公司的市场占有率均达到或超过了6%。

2021年全球网络安全软件行业竞争格局



2021年我国网络安全行业市场竞争格局

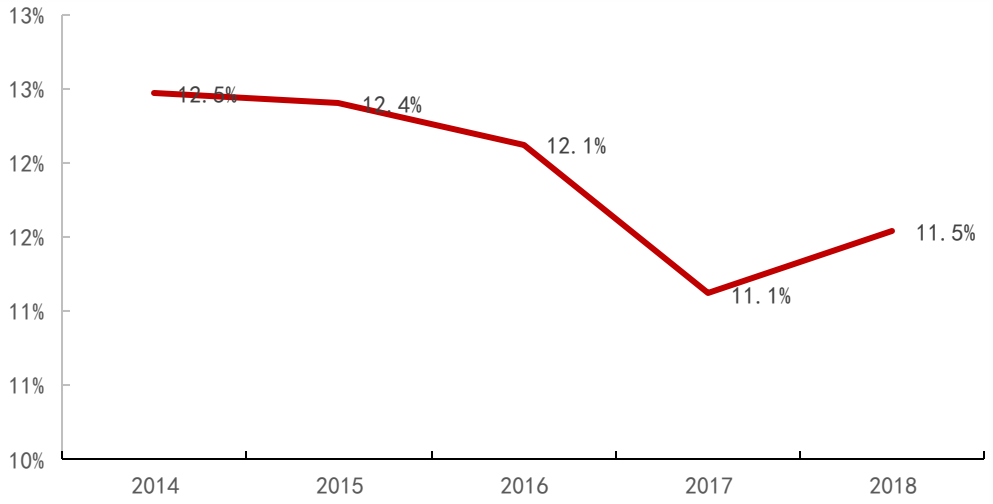


数据来源：Datanyze，中国网络安全产业联盟，，西南证券整理

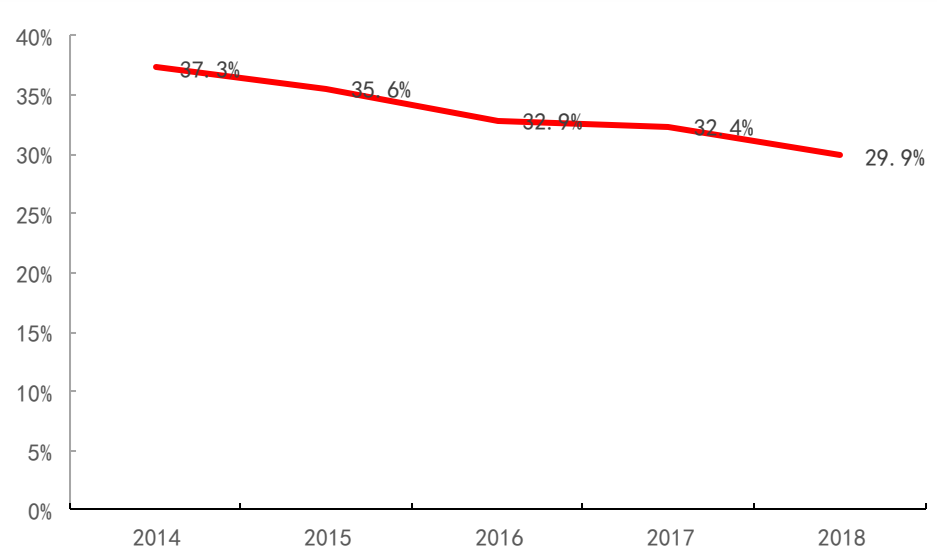
4 网络安全国内外对比—竞争格局

- 从市场格局上看，**国内外网络信息安全市场呈现高度分散的特点。**也就是说，**网络安全行业的发展不是带来行业集中度的提升，而是下降。**
- **全球Top5网络安全公司（Symantec、Cisco、PaloAltoNetworks、CheckPoint、Fortinet）**在整个网络安全市场里所占的份额在11%～12%，从全球网络安全行业的实际发展情况来看，**行业集中度很低，而且还有不断变低的趋势。**
- **国内Top5的网络安全公司（启明星辰、奇安信、卫士通、深信服、天融信）所占市场份额正在显著地持续下降。**与全球网络信息安全市场相比，虽然较全球的比例更高些，但中国Top5网络安全公司收入占行业整体收入的份额正在显著地逐年下降中，已从37.3%下降至29.9%。**行业集中度不高，网络信息安全产品同质性强，容易陷入激烈的竞争。**
- **未来，随着智慧城市、信息化、5G的落地，对IT公司的综合实力要求较高，从而为实力雄厚的IT公司提供了发展机会，市场集中度将上升。但是，作为一个小而美的市场，网络安全市场增速较为稳定，平均增速接近20%。**

全球Top5网络安全厂商营收占比



国内Top5网络安全厂商营收占比



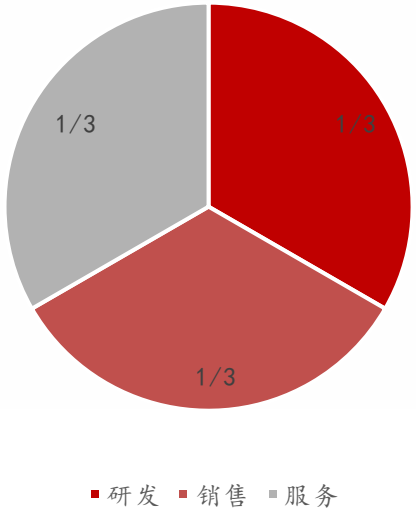
数据来源：Gartner，西南证券整理

4 网络安全国内外对比—人员构成

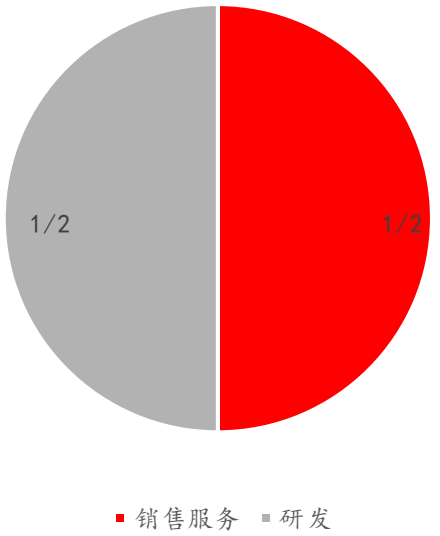
国内网络安全公司，**销售、研发、服务人员比例各占1/3**；**国外**网络安全公司，**研发人员比例占1/2，而销售和服务人员比例共占1/2。**

- **国内网络安全厂商人员构成中销售人员比例较高。**
  - 国内大多数客户**对安全的理解有限，产品或方案的选择能力缺失或只是为了应对监管要求**，所以竞争中**销售的能力成为了赢单的关键因素。**海外由于面对全球市场，边际效应相比国内更好，所以销售投入较少。
- **国外网络安全厂商人员构成中研发人员比例较高。**
  - 在**网络安全研发**方面，《白皮书》显示，我国主要网络安全上市企业研发投入普涨，但**研发费用率低于国际同业水平。**对比国外，以微软为例，庞大的业务安全和云计算服务平台安全性成为了微软所面临的巨大挑战。因此**微软在安全领域“大手笔”投入**：每**年在网络安全研发方面的投资超过10亿美元，汇集全球超3500名安全专家。**

国内网络安全公司人员构成



国外网络安全公司人员构成



数据来源：中国网络安全产业联盟，西南证券整理

目 录

1 网络安全客户采购驱动因素

2 网络安全行业发展趋势

3 网络安全核心细分领域

3.1 防火墙
3.2 数据安全
3.3 密码安全
3.4 身份与访问安全
3.5 零信任

4 网络安全行业国内外对比

4.1 产业生态
4.2 竞争格局
4.3 人员构成

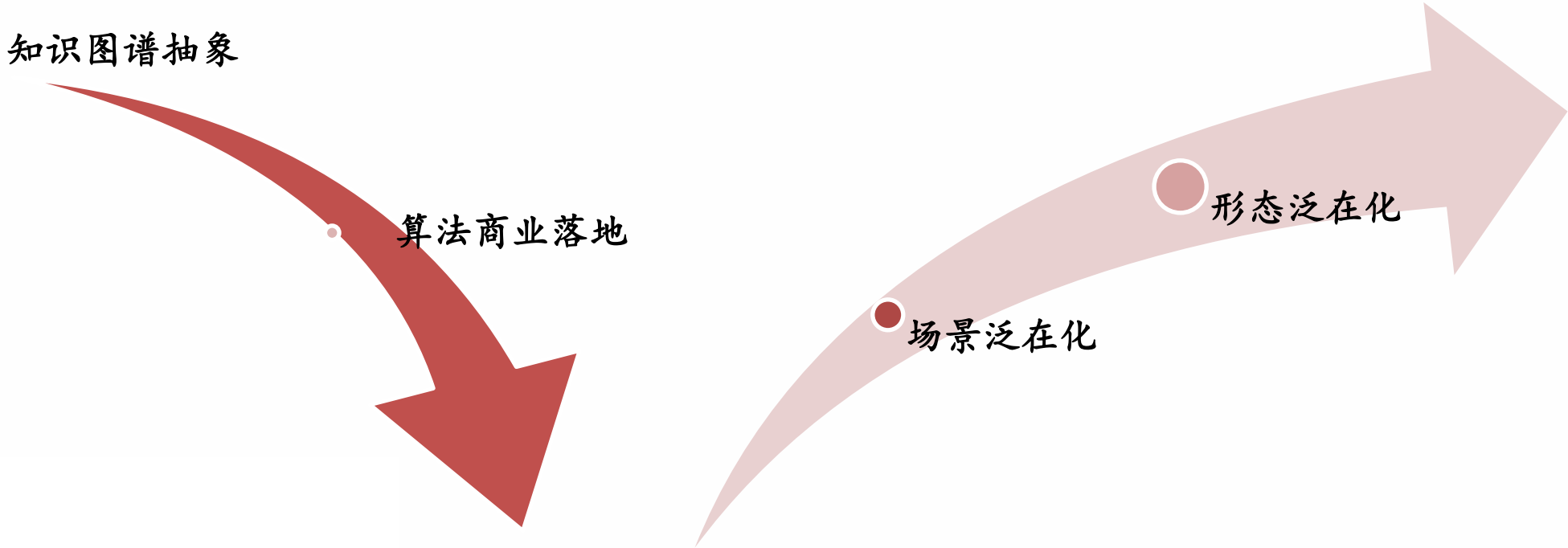
5 网络安全厂商未来核心竞争力

5 网络安全厂商未来核心竞争力

网络安全产业迎来爆发期，安全技术和产品创新发展，智能化成为必然趋势，智能化、主动化将成为竞争力关键。**未来网络安全厂商的核心竞争力主要反映在技术纵向深化和场景与形态横向拓展上。**

- **纵向来看，**如何实现对AI的应用是未来网安厂商竞争的关键点，这主要体现在两个方面：**1）知识图谱的抽象；2）相关算法的商业落地。**
- **横向来看，**未来**网络安全产品存在泛在化趋势**，如何进行**应用场景的拓展和产品形态的更新**也是未来网安厂商竞争的关键点。

未来网安厂商如何竞争？



信息来源：世界智能大会，Gartner等，西南证券整理

5 网络安全厂商未来核心竞争力

对AI技术的应用能力首先体现在对知识图谱的抽象能力上。

- **能否利用AI技术进行网络安全知识图谱抽象是未来网安厂商可否在竞争中胜出的重要能力。**随着攻防抵抗态势的升级，自动化、智能化规划技术与攻防技术的融合已成为网络安全技术发展的必然趋势之一，在网络安全智能化发展的过程中，**网络安全知识图谱构建已成为基础核心工作。**
- **安全知识图谱的智能化构建，**即安全知识图谱的抽象，是指利用机器学习、深度学习、认知智能等方法主动、智能地从海量数据中提取高价值的安全情报，完成本体构建、图谱构建、知识表示、图谱推理，进行自动化安全防御。
- **知识图谱**是实现认知智能的关键技术，**是实现机器认知智能的使能器。认知智能是知识图谱等知识工程技术发展的下一站**，是以知识图谱为代表的大数据知识工程突破自身局限、进一步完善的必经智能形态。

安全知识图谱技术趋势



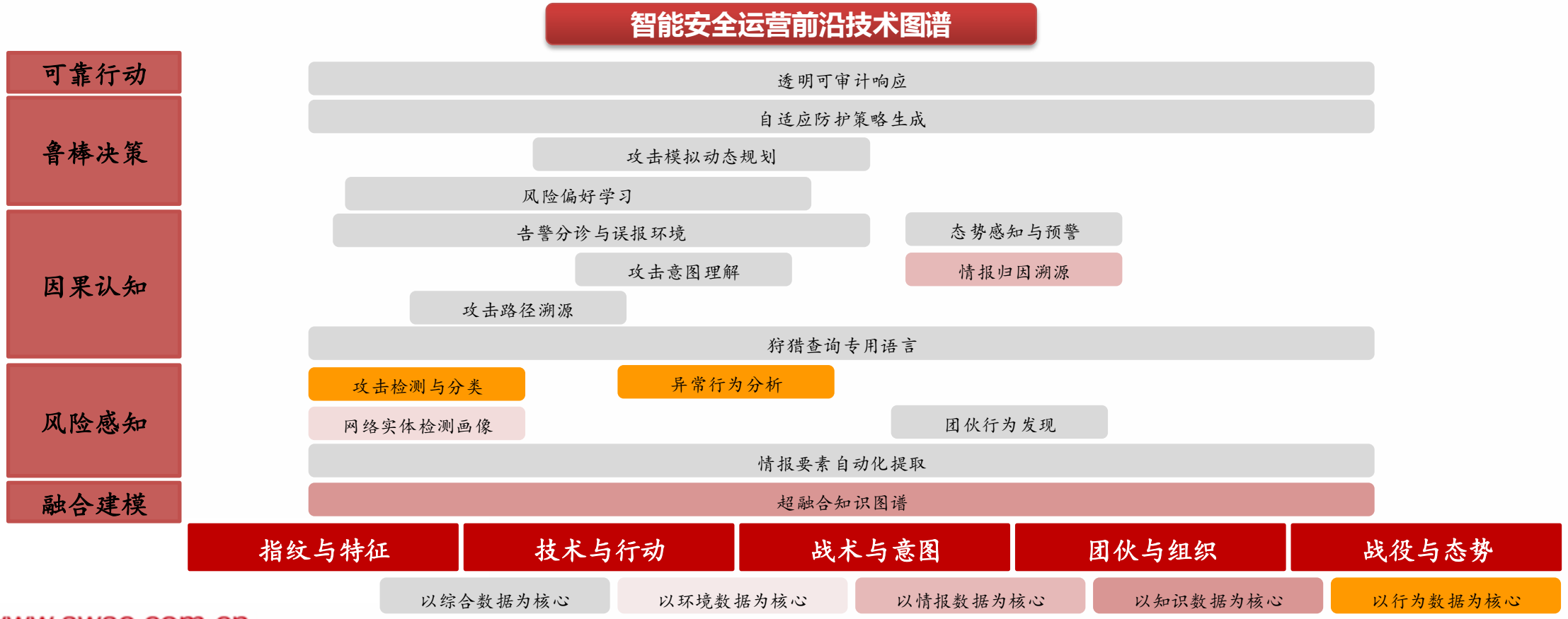
网安智能化发展趋势



信息来源：绿盟科技，天融信，复旦大学知识工场实验室等，西南证券整理

5 网络安全厂商未来核心竞争力

对AI技术的应用能力其次体现在准确有效进行算法商业落地的能力上。
未来，安全营运智能化成为必然趋势，流量分析、行为分析、样本分析、威胁关联、自动化响应等技术越来越多地采用了机器学习算法、图算法、强化学习算法，尽管如此，现阶段安全智能的发展水平，仍难以满足安全运营对威胁发现实时性与准确性、事件自动化溯源、风险决策自动化等多方面的要求，**如何将合适的算法应用在适当的场景下，解决客户最根本的痛点是未来网安厂商需求聚焦的研究方向。**



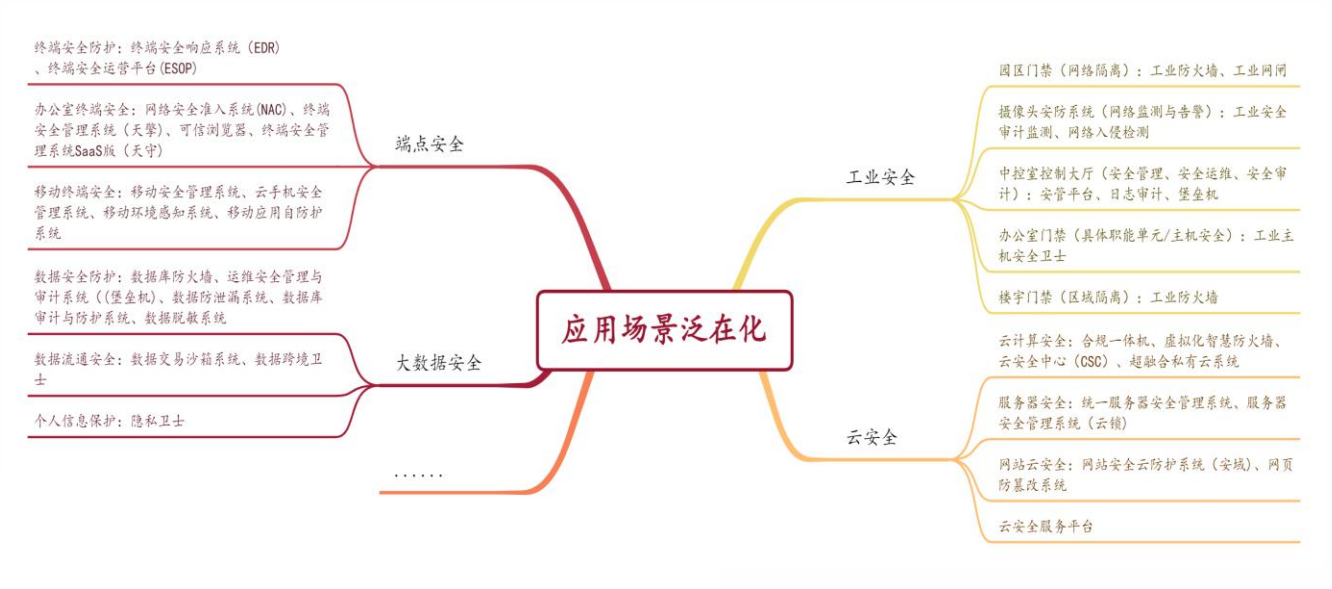
信息来源：《AISecOps智能安全运营技术白皮书》，西南证券整理

5 网络安全厂商未来核心竞争力

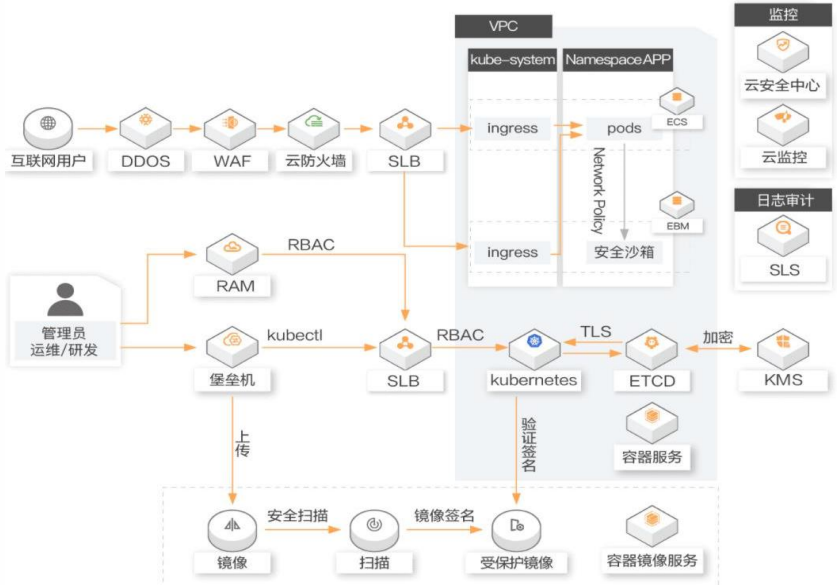
网络安全发展存在泛在化趋势，不论是应用场景和产品形态都显示出泛在化趋势。

- **应用场景上**，随着全球数字经济的蓬勃发展，网络安全与物联网、车联网、工业互联网、云计算、5G等多种场景和技术进行融合，全面、深刻地改变了网络安全防护体系面貌；随着未来区块链技术的发展，金融、证券、保险等领域以及供应链、知识产权保护、合同存证、审计、捐款追踪、积分管理等应用场景也将离不开网络安全的保护。
- **产品形态上**，出现了安全云化、容器云安全、智能化XDR等新形态。随着云计算在国内应用范围不断扩大，云计算业改变了安全产品销售模式和交付方式，越来越多的互联网企业、安全厂商开始探索用云的方式销售和交付安全产品，如天融信典型云安全产品有云WAF、云抗D、云安全资源池等。

未来网络安全产品应用场景的泛在化



云安全产品



信息来源：天融信，安恒信息，奇安信等，西南证券整理

5 网络安全厂商未来核心竞争力

“AI+安全”将带来利润、资源、效率等方面优势。

- ✓ **目前网络安全行业人工成本较高，**需要大量技术人员进行安全防御工作，导致整个行业毛利率很低，尤其产品硬件的毛利率不超过9%，**当AI赋能安全之后，人工成本将大大降低，毛利率将得到提升，例如托管云产品毛利率在80%以上。**
- ✓ **效率上，实现安全威胁的快速感知、主动捕获、关联预测、动态对抗，还支持轻量化、场景定制化、全局安全联动部署；**通过将AI应用到网络安全防护中，能够**实现对网络威胁的预先研判、智能防护和自动抵御，有效提升安全威胁检测、态势感知、应急处置和追踪溯源能力，实现安全防护技术的与时俱进。**
- ✓ **资源上，**提升资源的复用率，复用率越高，利润率越高。



信息来源：数字经济发布，至顶网，西南证券整理

西南证券
SOUTHWEST SECURITIES

分析师：王湘杰
执业证号： S1250521120002
电话：0755-26671517
邮箱：wxj@swsc.com.cn

分析师：叶泽佑
执业证号：S1250522090003
电话：13524424436
邮箱：yezy@swsc.com.cn

西南证券投资评级说明

报告中投资建议所涉及的评级分为公司评级和行业评级（另有说明的除外）。评级标准为报告发布日后6个月内的相对市场表现，即：以报告发布日后6个月内公司股价（或行业指数）相对同期相关证券市场代表性指数的涨跌幅作为基准。其中：A股市场以沪深300指数为基准，新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以恒生指数为基准；美国市场以纳斯达克综合指数或标普500指数为基准。

公司评级	买入：未来6个月内，个股相对同期相关证券市场代表性指数涨幅在20%以上
	持有：未来6个月内，个股相对同期相关证券市场代表性指数涨幅介于10%与20%之间
	中性：未来6个月内，个股相对同期相关证券市场代表性指数涨幅介于-10%与10%之间
	回避：未来6个月内，个股相对同期相关证券市场代表性指数涨幅介于-20%与-10%之间
	卖出：未来6个月内，个股相对同期相关证券市场代表性指数涨幅在-20%以下
行业评级	强于大市：未来6个月内，行业整体回报高于同期相关证券市场代表性指数5%以上
	跟随大市：未来6个月内，行业整体回报介于同期相关证券市场代表性指数-5%与5%之间
	弱于大市：未来6个月内，行业整体回报低于同期相关证券市场代表性指数-5%以下

分析师承诺

报告署名分析师具有中国证券业协会授予的证券投资咨询执业资格并注册为证券分析师，报告所采用的数据均来自合法合规渠道，分析逻辑基于分析师的职业理解，通过合理判断得出结论，独立、客观地出具本报告。分析师承诺不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接获取任何形式的补偿。

重要声明

西南证券股份有限公司（以下简称“本公司”）具有中国证券监督管理委员会核准的证券投资咨询业务资格。

本公司与作者在自身所知情范围内，与本报告中所评价或推荐的证券不存在法律法规要求披露或采取限制、静默措施的利益冲突。

《证券期货投资者适当性管理办法》于2017年7月1日起正式实施，本报告仅供本公司签约客户使用，若您并非本公司签约客户，为控制投资风险，请取消接收、订阅或使用本报告中的任何信息。本公司也不会因接收人收到、阅读或关注自媒体推送本报告中的内容而视其为客户。本公司或关联机构可能会持有报告中提到的公司所发行的证券并进行交易，还可能为这些公司提供或争取提供投资银行或财务顾问服务。

本报告中的信息均来源于公开资料，本公司对这些信息的准确性、完整性或可靠性不作任何保证。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可升可跌，过往表现不应作为日后的表现依据。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告，本公司不保证本报告所含信息保持在最新状态。同时，本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本报告仅供参考之用，不构成出售或购买证券或其他投资标的要约或邀请。在任何情况下，本报告中的信息和意见均不构成对任何个人的投资建议。投资者应结合自己的投资目标和财务状况自行判断是否采用本报告所载内容和信息并自行承担风险，本公司及雇员对投资者使用本报告及其内容而造成的一切后果不承担任何法律责任。

本报告及附录版权为西南证券所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制和发布。如引用须注明出处为“西南证券”，且不得对本报告及附录进行有悖原意的引用、删节和修改。未经授权刊载或者转发本报告及附录的，本公司将保留向其追究法律责任的权利。

西南证券 SOUTHWEST SECURITIES

西南证券研究发展中心

西南证券研究发展中心

上海

地址：上海市浦东新区陆家嘴东路166号中国保险大厦20楼

邮编：200120

北京

地址：北京市西城区金融大街35号国际企业大厦A座8楼

邮编：100033

深圳

地址：深圳市福田区深南大道6023号创建大厦4楼

邮编：518040

重庆

地址：重庆市江北区金沙门路32号西南证券总部大楼

邮编：400025

西南证券机构销售团队

区域	姓名	职务	座机	手机	邮箱
上海	蒋诗烽	总经理助理、销售总监	021-68415309	18621310081	jsf@swsc.com.cn
	崔露文	高级销售经理	15642960315	15642960315	clw@swsc.com.cn
	王昕宇	高级销售经理	17751018376	17751018376	wangxy@swsc.com.cn
	薛世宇	销售经理	18502146429	18502146429	xsy@swsc.com.cn
	汪艺	销售经理	13127920536	13127920536	wyyf@swsc.com.cn
	岑宇婷	销售经理	18616243268	18616243268	cyryf@swsc.com.cn
	陈阳阳	销售经理	17863111858	17863111858	cyyyf@swsc.com.cn
	张玉梅	销售经理	18957157330	18957157330	zymyf@swsc.com.cn
	李煜	销售经理	18801732511	18801732511	yfliyu@swsc.com.cn
北京	李杨	销售总监	18601139362	18601139362	yfly@swsc.com.cn
	张岚	销售副总监	18601241803	18601241803	zhanglan@swsc.com.cn
	杜小双	高级销售经理	18810922935	18810922935	dxsyf@swsc.com.cn
	王一菲	销售经理	18040060359	18040060359	wyf@swsc.com.cn
	王宇飞	销售经理	18500981866	18500981866	wangyuf@swsc.com
	巢语欢	销售经理	13667084989	13667084989	cyh@swsc.com.cn
广深	郑龑	广深销售负责人	18825189744	18825189744	zhengyan@swsc.com.cn
	杨新意	销售经理	17628609919	17628609919	yxy@swsc.com.cn
	张文锋	销售经理	13642639789	13642639789	zwf@swsc.com.cn
	陈韵然	销售经理	18208801355	18208801355	cyryf@swsc.com.cn
	龚之涵	销售经理	15808001926	15808001926	gongzh@swsc.com.cn
	丁凡	销售经理	15559989681	15559989681	dingfyf@swsc.com.cn