2021 年 7 月 13 日

滴滴事件定性、行动计划定量，网安开启长牛

计算机行业

核心逻辑：

近期网络安全利好催化不断，其中尤以***《网络安全法》***对于滴滴的安全审查事件和***《网络安全产业高质量发展三年行动计划(2021-2023 年)(征求意见稿)》***（后简称《行动计划》）的出台最为重要。前者定性网安（大数据安全）的战略定位，后者定量描绘行业扩容趋势与远期产业空间。

滴滴事件：数据安全/审查大幕拉开，安全产业站上风口。本次滴滴事件凸显我国数据安全的隐患。随着监管下场开启全面整顿，数据安全/审查大幕拉开。“大数据安全”是当前个人、企业、政府一致的安全重灾区。个人层面来看，私人信息泄露可能造成重大财产损失甚至危及人身安全。政企层面来看，关键数据资产的泄露可能招致国家网络信息系统被攻击的危险，尤其是针对关键性基础设施的网络攻击会导致重大国家安全事故。判断，**以本次滴滴事件为界限，我们将正式从“网络空间安全”上半场（关注边界安全，例如防火墙、VPN 等，步入下半场（聚焦内容安全及数据安全，例如态势感知、隐私安全等）。**

《行动计划》定量，10%划定打开数千亿级空间。另一方面，上海经信委和工信部先后两次公开宣布网安 IT 投入占比，从定量的层面框定了未来网安行业的基本盘——政府与企业侧预算。工信部在《行动计划》中明确：至 2023 年网络安全产业规模将超过2500亿元、年复合增速超过15%，同时明确电信等重点行业网络安全投入占信息化投入比例达 10%。**1）需求侧来看：**如果 2023 年实现 2500 亿元的产业空间，且年复合增速 15%，则倒推 2021 年产业规模是 1600-1700 亿。**2）供给侧来看：**就提供的安全产品/服务供给来看，CCID 数据显示 2019-2021 年我国网络信息安全市场规模将由 608 亿元增加至 927 亿元，CAGR 为 23.5%。**3）线性外推：**若结合两个10%的网安IT投入占比划定，并线性外推至全部政府、企业客户（判断符合顶层规划思路），则 2021 年安全供需缺口 = 安全厂商业务扩容空间 = 700-800 亿元，产业机遇不言自明。当然，考虑到：大G/大B的预算调整节奏、现实的政府预算压力等，**判断扩容的周期应当并不局限于当前的1-2年，换而言之，本轮政策对于安全行业而言更接近长期预算中枢的抬升，亦即推动行业迎来长牛。**

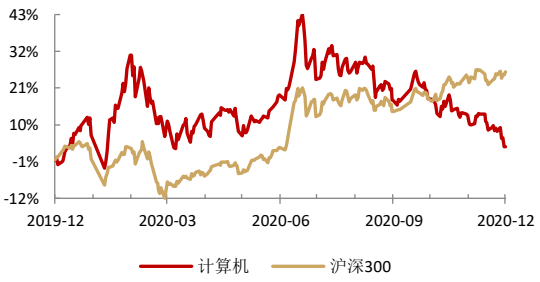
引申思考：数据反垄断，网安或是新基建？平台垄断实为**“双重垄断”**，即表面是在某一商业领域形成业务垄断，实质是对某一领域的个人/企业/甚至政府单位形成数据垄断和闭环。当今社会，数据资产绝不仅仅是一个商业问题，更是涉及主权安全/战略的问题，预计未来数据反垄断立法和监管都将不断推进，对于监管机构的赋能输出（数据新基建）成为重要增量。

投资建议：梳理可知，三类安全公司真正受益：**1）全能型厂商：整体性受益本次事件/政策红利。**指具备齐全安全产品线的

评级及分析师信息

行业评级：推荐

行业走势图



分析师：刘泽晶
邮箱：liuzj1@hx168.com.cn
SAC NO：S1120520020002
联系电话：

分析师：刘忠腾
邮箱：liuzt1@hx168.com.cn
SAC NO：S1120520050001
联系电话：0755-82533391

分析师：孔文彬
邮箱：kongwb@hx168.com.cn
SAC NO：S1120520090002
联系电话：

厂商，至少在两到三个领域跻身市占率第一梯队，包括**奇安信、深信服、启明星辰、绿盟科技、天融信**五家；**2）专精型厂商：局部性受益本次事件/政策红利。**指其他细分安全领域的龙头，多为深耕单一领域多年的单项冠军，包括但不限于**安恒信息、格尔软件、信安世纪、中孚信息**等；**3）审查型厂商，特定受益厂商，或是本次事件/政策红利最大预期差。**网络空间治理近年受到高度关注，该产业下游往往为政法系统单位，具有鲜明的网络执法属性，该细分领域内主要参与者包括但不限于**美亚柏科、中新赛克**等。

综合而言，坚定看好全能型厂商中的双龙头**奇安信 + 深信服**，同时大数据安全专精厂商**安恒信息**以及安全审查赛道的**美亚柏科**明确受益。

风险提示：网安行业政策推进不及预期，云/态势感知等创新业务进展不及预期。

盈利预测与估值

重点公司											
股票代码	股票名称	收盘价（元）	投资评级	EPS（元）				P/E			
				2020A	2021E	2022E	2023E	2020A	2021E	2022E	2023E
300454.SZ	深信服	298.01	买入	2	2.8	3.7	4.9	136	98	74	56
688561.SH	奇安信-U	122.76	买入	-0.50	0.2	0.7	1.72	-255	448	128	52

资料来源：Wind，华西证券研究所

正文目录

目录

1. 引言：系列事件催化，网安长牛启航

近期网络安全利好催化不断，其中尤以《网络安全法》对于滴滴的安全审查事件和《网络安全产业高质量发展三年行动计划(2021-2023 年)(征求意见稿)》(后简称《行动计划》)的出台最为重要。**前者定性网安（大数据安全）的战略定位，后者定量描绘行业扩容趋势与远期产业空间。**

两者形成合力，一扫市场对于网络安全行业的三大担忧：

1）对成长性/持续性的担忧，在 HW 和信创以外难寻其他新增长点；

2）对政府侧/企业测的短期投入力度的担忧；

3）对于行业远期天花板的担忧。

在此时点，我们通过对滴滴事件、《网安产业行动计划》、数据反垄断三大现象进行分类解读，试图明确行业新的景气周期与核心收益厂商。

2. 滴滴事件定性，网安获战略新定位

2.1. 滴滴事件：监管重拳出击的背后，暗流涌动

1）事件：滴滴“突击”赴美上市。

国内网约车平台巨头滴滴于 2021 年 6 月 30 日在美股“突击”上市，网信办随即在 7 月 2 日发出公告，启动对滴滴的网络安全审查，同时停止新的用户的注册。此后数日，系列监管措施进一步出台，对“滴滴出行”APP 和其他滴滴系 APP 进行全网下架，并开展全方位调研。

图表 1　滴滴出行 App 下架通报

资料来源：国家互联网信息办公室、华西证券研究所

图表 2　针对运满满、货车帮、BOSS 直聘的审查公告

资料来源：网信办，华西证券研究所

2）监管：监管政策密集出台，时间轴梳理如下：

- 7 月 2 日，国家网信办官网发布公告，网络安全审查办公室宣布对滴滴出行启动网络安全审查。
- 7 月 4 日，国家网信办通知应用商店下架“滴滴出行”App，要求滴滴出行科技有限公司严格按照法律要求，参照国家有关标准，认真整改存在的问题，切实保障广大用户个人信息安全。
- 7 月 5 日，网络安全审查办公室宣布对“运满满”、“货车帮”、“BOSS 直聘”实施网络安全审查，审查期间停止新用户注册，对个人信息安全保护的监管措施逐渐走向常态化。
- 7 月 9 日，国家网信办宣布经检测核实，“滴滴企业版”等 25 款 App 存在严重违法违规收集使用个人信息问题。通知应用商店下架此 25 款 App，各网站、平台不得为已在应用商店下架的 App 提供访问和下载服务。
- 7 月 10 日，国家网信办发布关于《网络安全审查办法（修订草案征求意见稿）》公开征求意见的通知，要求掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

图表 3　此次下架整顿的 25 款滴滴系 APP

序号	App 名称	属地	主办单位
1	滴滴企业版	北京市	北京小桔科技有限公司
2	滴滴车主	北京市	北京小桔科技有限公司
3	滴滴顺风车	北京市	北京小桔科技有限公司
4	Uber 优步中国	北京市	北京小桔科技有限公司
5	滴滴司机部落	北京市	北京小桔科技有限公司
6	滴滴司机-出租车版	北京市	北京小桔科技有限公司
7	滴滴代驾司机	北京市	北京小桔科技有限公司
8	桔视记录仪	北京市	北京小桔科技有限公司
9	滴滴金融	北京市	北京小桔科技有限公司
10	谷雨	北京市	北京小桔科技有限公司
11	专车司机助手	北京市	北京小桔科技有限公司
12	滴滴敬老版	北京市	北京小桔科技有限公司
13	滴滴货运司机	北京市	北京小桔科技有限公司
14	滴滴配送	北京市	北京小桔科技有限公司
15	滴滴商户	北京市	北京小桔科技有限公司
16	蓝鲸	北京市	北京小桔科技有限公司
17	滴滴护航	北京市	北京小桔科技有限公司
18	D-Chat	北京市	北京小桔科技有限公司
19	小桔智慧	北京市	北京小桔科技有限公司
20	滴滴小巴司机	北京市	北京小桔科技有限公司
21	滴滴公交	北京市	北京小桔科技有限公司
22	LIMO	北京市	北京小桔科技有限公司
23	小桔加油收银台商家版	北京市	北京小桔科技有限公司
24	桔视智行	北京市	北京小桔科技有限公司
25	滴滴司机助手	北京市	北京小桔科技有限公司

资料来源：国家网信办、华西证券研究所

3）透过现象看本质：中美博弈、暗流涌动

此次针对滴滴的大力度整顿，看似突发应对之举，实则是中美双方在金融 & 科技领域的又一次交锋，可谓暗流涌动已久。

2020 年 5 月，美国，《外国公司问责法案》提出。《外国公司问责法案》要求，在美上市的外国企业要向美国证券交易委员会（SEC）提交审计底稿。对于掌握大量关键数据的企业而言，这其实意味着国家层面的数据安全风险。《外国公司问责法案》的提出之后，在美上市的中概股大跌，网易、京东、B 站等企业纷纷在中国香港二次上市，尽管美国资本市场构成了不小冲击，但美国国会还是在 2020 年 12 月顺利通过了《外国公司问责法案》。后续来看，新任的拜登政府也没有在这一层面做出任何让步，反而美国证监会还在 2021 年 3 月 24 日进一步发布《外国公司问责法案》的实施细则。

2020年6月，中国，《数据安全法》审议。《外国公司问责法案》提出后的次月，即 2020 年 6 月全国人大常委会第一次审议《数据安全法》草案，而后在 7 月面向社会公开征求意见。2021 年 6 月 10 日，全国人大常委会正式通过了《数据安全法》，并将于 9 月正式实施。其中第 36 条明确提出："非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。"

值得注意的是，这两部法律都是2020年公布，但2021年才逐步实施，这就留下一个"灵活"的窗口期。对于中概股而言，《外国公司问责法案》要求其向美国 SEC 提交审计底稿，而《数据安全法》则要求非经批准不得提供数据，冲突不言自明。但是考虑到两套法律都是 2020 年公布、2021 年开始逐步实施，于是留下一个"灵活"的窗口期。据不完全统计，2021 年上半年共有 11 家中国互联网企业上市。其中市值超过 100 亿美元的有 5 家：滴滴、满帮、BOSS 直聘、快手、京东物流。值得注意的是，3 家赴美上市（而非中国香港上市）的企业均已经遭到了网络安全审查。同时指出，3 家的上市时间也恰好处在《数据安全法》通过（6 月 10 日）后。

图表 4　2021 年海外资本市场上市的中国科技公司（部分）

证券简称	上市时间	交易所
快手-W	2月5日	港交所
滴滴出行(DIDI)	6月30日	纽交所
京东物流	5月28日	港交所
满帮集团(FULL TRUCK ALLIANCE)	6月22日	纽交所
BOSS直聘	6月11日	纳斯达克
叮咚买菜(DINGDONG)	6月29日	纽交所
知乎(ZHIHU)	3月26日	纽交所
万物新生(AIHUISHOU INTL)	6月18日	纽交所
水滴公司(WATERDROP)	5月7日	纽交所
每日优鲜(MISSFRESH)	6月25日	纳斯达克
怪兽充电(SMART SHARE GLOBAL)	4月1日	纳斯达克

资料来源：wind、华西证券研究所

2.2. 数据安全/审查大幕拉开，安全产业站上风口

我们认为，本次滴滴事件凸显了我国数据安全的极大隐患。**随着监管下场开启全面整顿，数据安全/审查大幕已经拉开，并将直接推动泛网络安全行业景气度上行，细分龙头有望持续受益。**

从安全产业自身来看：随着信息技术的快速演进，全球数据泄露等网络安全事件频繁发生，造成重大损失。根据 CCID 发布《2019 年网络安全发展白皮书》，全球安全漏洞数量和严重性创下历史新高；而中国重大网安事件也几乎每月必现。据 Cybersecurity Ventures 预测，到 2021 年全球因网络安全事件导致的损失将高达 6 万亿美元/年。

就细分领域而言，"大数据安全"正在成为当前个人、企业、政府一致的安全重灾区。近几年移动互联网、工业互联网的快速发展极大拓展了网络攻击的渠道，攻击模式急剧多元/复杂化，数据安全问题无处不在：

- **个人层面来看**，网安问题会带来私人信息泄露，进而威胁生命、财产安全。

- **政企层面来看**，关键数据资产的泄露可能招致国家网络信息系统被攻击的危险，尤其是针对关键性基础设施的网络攻击会导致重大国家安全事故。

在此背景下，网络安全正式步入“网络空间安全”的下半场。根据安全牛披露，我国网安发展历程可分为起源期、萌芽期、成长期和加速期四个时期，分别对应通信加密时代、计算机安全时代、信息安全时代和网络空间安全时代。随着通信技术演进及移动互联网普及，企业信息化程度持续提升，自动化和远程办公的需求激增，网安关注点逐渐延伸至网络空间本身，2015 年开始网安行业正式进入“网络空间安全”时代。关注网络空间安全的两个核心领域：

- **前半场：**关注网络边界安全，例如防火墙、VPN 等；
- **后半场：**聚焦内容安全及数据安全，例如态势感知、云安全、隐私安全等。

判断，以本次滴滴事件为界限，我们将正式步入网络空间安全时代的下半场。

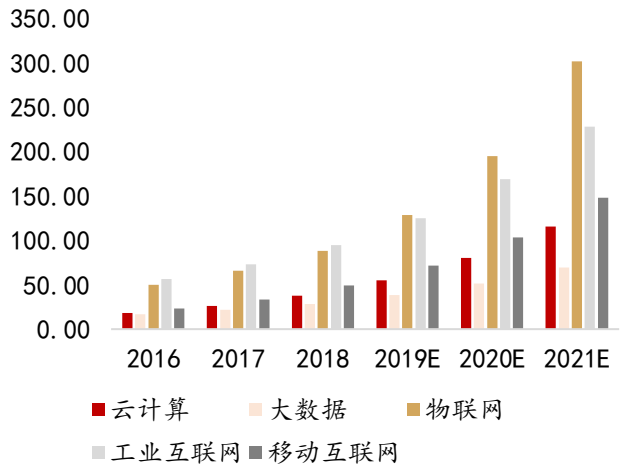
图表 5　我国网络安全发展四阶段

资料来源：安全牛、华西证券研究所

大数据安全新兴安全的重要分支，态势感知以外，隐私安全、零信任也将成为新的热点技术。当前来看，“云大物工移”相关安全领域是最有潜力的网安新兴市场，在云计算、大数据、物联网、工业互联网、移动互联网等前沿技术的驱动下，网络安全行业应用场景不断扩展。

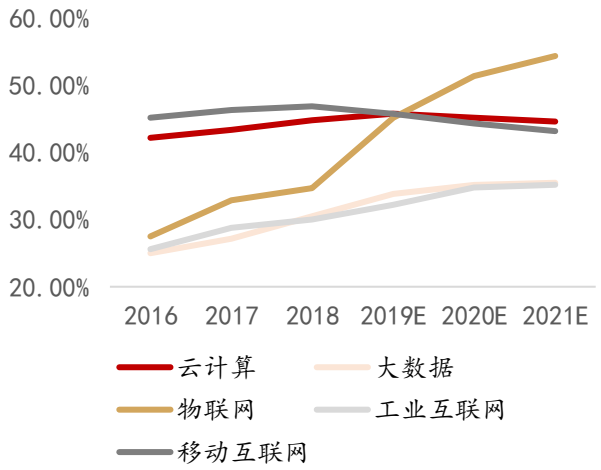
1）根据 CCID 预测，到 2021 年我国云计算安全、大数据安全、物联网安全、工业互联网安全、移动互联网安全市场规模分别为 115.7 亿元、69.7 亿元、301.4 亿元、228 亿元、148.2 亿元，未来 3-5 年各细分领域年均复合增速均超过 30%。在几类新兴安全产品赛道中，大数据安全体量相对有限，但这与个人对于隐私数据、企业/政府对于业务数据的重视程度、保护诉求高度关联。随着滴滴事件敲响警钟，G 端/B 端/C 端用户必将极大提升对于互联网平台的大数据安全的重视程度，赛道拓展空间巨大。

图表 6 “云大物工移“细分市场规模及预测（亿元）



资料来源：CCID、华西证券研究所

图表 7 “云大物工移“细分市场规模增速及预测



资料来源：CCID、华西证券研究所

2）过去几年间，态势感知是大数据安全的绝对热点。态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。2016 年 419 网络安全和信息化工作座谈会上，习近平总书记提出“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。数世咨询数据显示，2019 年国内态势感知市场规模约 32 亿元，预计 2021 年将增长至 54 亿元。

图表 8 部分新兴领域领导厂商（2018）

新兴技术领域	典型厂商
云安全	阿里云、知道创宇、 安恒信息 、绿盟科技、启明星辰 、奇安信
大数据安全	**奇安信、 安恒信息、启明星辰 、 亿赛通 、 绿盟科技 、 美亚柏科 、 明朝万达**
物联网安全	奇安信、 青莲云 、 绿盟科技 、 阿里云 、 华为
工业互联网安全	威努特、 天地合兴 、 海天炜业 、 力控华康 、 长扬科技
移动互联网安全	梆梆安全、 爱加密 、娜迦信息、 通付盾
量子通信安全	国盾量子 、 问天量子、 神州信息 、中国有线 、 科华恒盛 、 蓝盾股份 、 阿里巴巴
态势感知	**奇安信 、 安恒信息 、 启明星辰 、 亚信安全 、 安博通**
威胁情报	ThreatBook 、 奇安信 、 威胁猎人 、 安天 、 白帽汇
区块链网络安全	知道创宇 、 白帽汇 、 BugX 、 成都链安 、 慢雾科技 、 Halo Block

资料来源：CCID、华西证券研究所

3）未来新的大数据安全更多将来自于隐私安全/合规、数据交易、零信任等。业内头部厂商已经推出相关产品：如奇安信的隐私卫士，是一款支持安卓和苹果 IOS 两大系统移动应用隐私合规检测与分析的系统、又如安恒信息的 Ailand 数据安全岛平台致力于解决数据共享的信任和隐私保护问题等等。判断随着新产品的落地及渗透带来用户习惯的加速转变，新场景的大数据安全需求将进一步释放。

3.《行动计划》定量，两个 10%打开数千亿级空间

滴滴事件并不是催化近期网安行业的唯一因素，上海经信委和工信部先后两次公开宣布网安 IT 投入占比，从定量的层面框定了未来网安行业的基本盘——政府与企业侧预算。

1）第一个 10%：近期在上海召开的全球人工智能大会上，上海经信委宣布，其正和网信办协商在后续的网安安全产业行动计划中，进一步明确政府和公共事业单位在网络安全上的投入比例不低于 10%。

2）第二个 10%：工信部在《网络安全产业高质量发展三年行动计划(2021-2023 年)(征求意见稿)》中提出，至 2023 年网络安全产业规模将超过 2500 亿元、年复合增速超过 15%，同时明确电信等重点行业网络安全投入占信息化投入比例达 10%。

本次比例划线将直接以政策驱动力打开需求侧空间：

需求侧来看：如果 2023 年实现 2500 亿元的产业空间，且年复合增速 15%，则倒推 2021 年产业规模是 1600-1700 亿。

供给侧来看：就提供的安全产品/服务供给来看，CCID 数据显示 2019-2021 年我国网络信息安全市场规模将由 608 亿元增加至 927 亿元，CAGR 为 23.5%。

即：若结合两个 10%的网安 IT 投入占比划定，并**线性外推至全部政府、企业客户（判断符合顶层规划思路），则 2021 年安全供需缺口 = 安全厂商业务扩容空间 = 700-800 亿元，**产业机遇不言自明。

当然，考虑到：**1）大 G/大 B 的预算调整节奏；2）现实的政府预算压力（尤其 2021 年）；3）网安 IT 比例划定对于企业的强制**性，扩容的周期应当并不局限于当前的 1-2 年，换而言之，本轮政策对于安全行业而言更接近长期预算中枢的抬升，**亦即推动行业迎来长牛。**

就行业增长驱动力来看，自上而下的三类政策驱动力将帮助网安厂商更快地消化预算中枢抬升带来的增量业务空间。

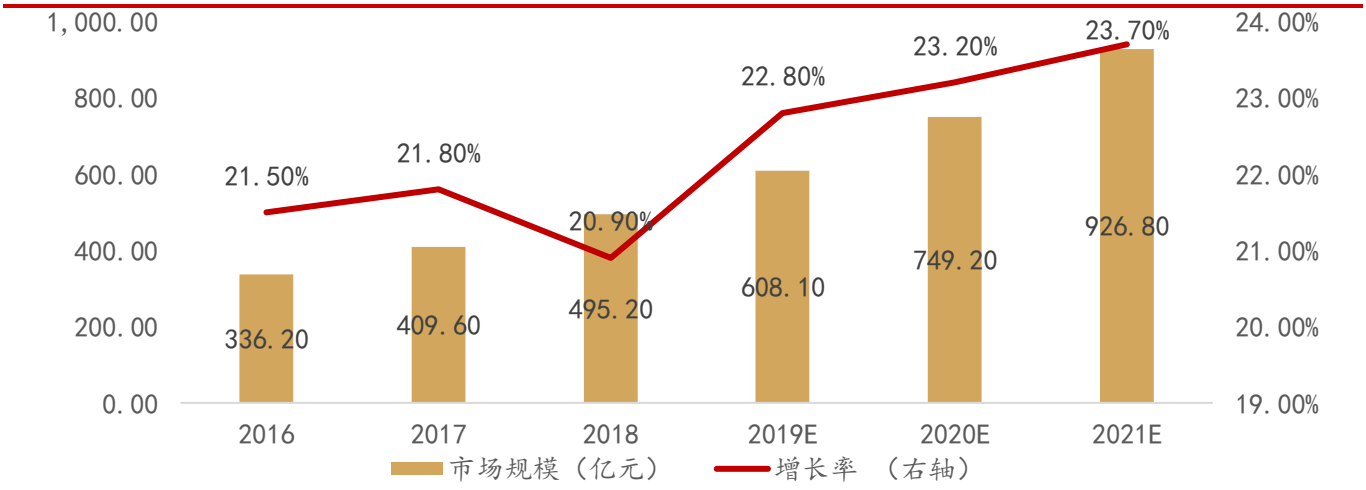
1）通过等保 2.0 等进行合规检查；

2）通过攻防实战对抗（HW）检验“成绩单”；

3）鼓励各地 G 端推动大数据新基建（基于安全/数据审查）。

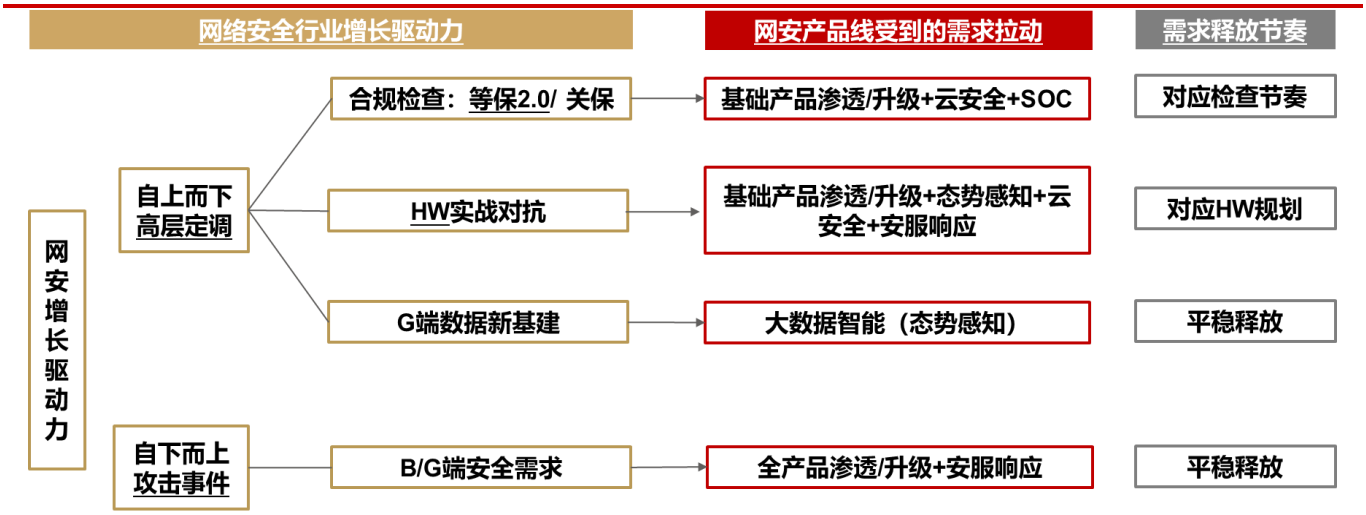
2020 年以来，等保 2.0 合规检查和 G 端大数据新基建均承压严重，主要原因仍是政府财政向抗疫事项倾斜，安全类预算整体缩减，此两类需求正在 2021 年催生大量新的订单需求。

图表 9　2016-2021 年我国网络安全市场规模与增长



资料来源：CCID、华西证券研究所

图表 10　当前我国网络安全行业增长驱动力



资料来源：CCID、华西证券研究所

以等保 2.0 为例，其在 2021-22 年的落实有望推动网安相关 IT 投入持续升级。信息安全等级保护是对信息和信息载体，按照重要性等级分级别进行保护的政策安排，是我国网络空间安全保障体系的重要支撑；2019 年 5 月 13 日《信息安全技术网络信息安全等级保护基本要求》国家标准正式发布，并于 2019 年 12 月 1 日正式实施，标志着我国网络安全等级保护工作正式进入“2.0 时代。整个等保 2.0 以新的检查要求驱动新产品的采购，各单位为了满足等保测评分数以备案成功，往往会依照针对性新增采购。新增要求项集中在入侵防范、恶意代码防范、集中管控、安全审计等方面。此外 SOC 以及态势感知已经成为了新检查重点。

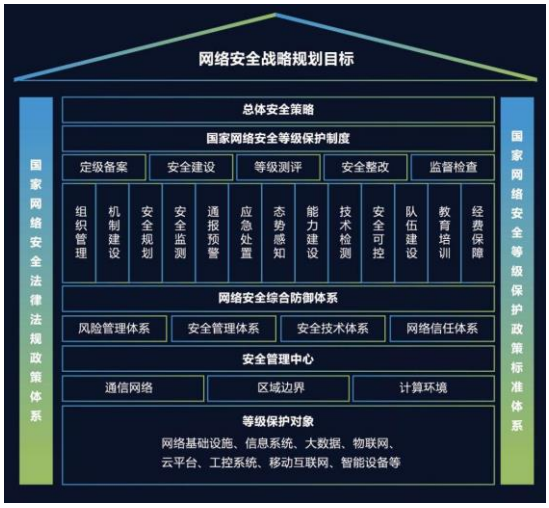
除此以外，实战攻防对抗（HW）的进一步扩容也是后续年份的重要看点。其对于国家网络安全体系化建设的积极意义已经在近年显露无疑，当前仍有进一步扩容趋势。预计未来 HW 将结合本次滴滴事件的监管导向，进一步聚焦大数据安全领域，将新安全需求 & 增量预算转化为产业红利。

图表 11 等保 2.0 vs 等保 1.0

	等保1.0	等保2.0
保障体系	被动防御：一个中心三重防护（防火墙、入侵检测、防病毒），以防为主	全方面主动防御：事前、事中、事后；感知预警、动态防护、安全监测、应急响应等
定级对象	信息系统	基础信息网络、工业控制系统、云计算平台、物联网、移动互联网、其他网络、大数据等多个系统
评测周期	三级的每年一次、四级的半年一次	三级以上系统每年一次
评测及格分	60分以上	75分以上
技术要求	包括技术要求（物理安全、网络安全、主机安全等）和管理要求（安全管理机构、安全管理制度、人员安全管理等）共290项	更新为技术要求（安全物理环境、安全通信网络、安全计算环境等）和管理要求（安全建设管理、安全运维管理、安全管理机构和人员等）共232项
其他新增要求	-	新增对新型网络攻击行为防护和个人信息保护等新要求：新增入侵防范（防火墙、IDS、IPS等）、恶意代码防范（邮件防护）、集中管控（VPN、堡垒机、终端安全软件、SOC/态势感知等）、安全审计（日志审计）等

资料来源：IDC、华西证券研究所

图表 12 等保 2.0 战略框架



资料来源：IDC、华西证券研究所

4. 引申思考：数据反垄断，网安或是新基建？

滴滴事件对于数据安全的定调、以及顶层对于网安 IT 投入比例的划定，已经在极大程度上明确了行业的景气度。**但我们认为，除此之外，滴滴事件还带来一个关于“数据反垄断”的引申思考，同样与网安厂商密切相关。**

滴滴事件带来的一个更深远的影响，就是对互联网平台巨头的数据反垄断。**判断随着高层进一步加强对数据垄断监管，并加码数据治理。**事实上，早在本次滴滴事件以前，我们在 2020 年 11 月的报告《醉翁何意？科技巨头反垄断影响分析》中就曾重点比较中美两国的反垄断浪潮，并总结共性。

1）美国反垄断：2020 年针对平台型科技巨头开始诉讼，为历史上第三轮反垄断浪潮。

美股市值是衡量其科技巨头垄断地位的重要指标。1980 年至今美股市值 Top 10 的美国公司不断变化，聚焦科技公司，我们认为三个变化值得关注：

1）科技巨头持续兴衰更迭，千禧年以前 IBM、AT&T 雄据榜单；千禧年以后思科、Intel、微软崛起接过大旗；近十年来看 FAMGA 是新龙头。

2）从数量上来看，传统科技巨头市值走弱后，数量更多、市值更大的新科技巨头形成，虽有巨头更迭，科技整体渐强。

3）从性质上来看，40 年间新巨头的属性由硬变软，从硬件与基础设施层面逐步迈向创新空间更大的软件、互联网。

图表 13　1980-2019 市值最大的美国公司

	1980	1990	2000	2010	2019
1	IBM	IBM	General Electric	Exxon Mobil	Microsoft
2	AT&T	Exxon	Exxon Mobil	Apple	Amazon
3	Exxon	General Electric	Pfizer	Microsoft	Apple
4	Amoco	Philip Morris	Citigroup	Berkshire Hathaway	Google
5	Schlumberger	Shell Oil	Cisco Systems	General Electric	Facebook
6	Shell Oil	Bristol-Myers Squibb	Wal-Mart	Wal-Mart	Berkshire Hathaway
7	Mobil	Merck	Microsoft	Google	Johnson & Johnson
8	Chevron	Wal-Mart	AIG	Chevron	JP Morgan Chase
9	Atlantic Richfield	AT&T	Merck	IBM	Visa
10	General Electric	Coca-Cola	Intel	Procter & Gamble	Exxon Mobil

Source: ETF Database, Visual History of the S&P 500, for 1980-2010; Finviz.com for 2019, data from May 16, 2019.

资料来源：SIFL，思想库报告、华西证券研究所

复盘历史，判断 1980 年至今共美国有三轮大的“反垄断”制裁。

1）80 年代针对 AT&T 和 IBM 的制裁，规模大、力度重，带来通信和计算机两个领域的 20 年繁荣。

2）2000 后，微软的“IE & Windows 绑定”模式受到制裁，同样催生浏览器新业态，谷歌等新巨头应运而生，20 年来软件生态逐步开放。

3）2020 年针对多家科技巨头的听证会正是新一轮“反垄断”制裁的开始。

本轮“反垄断”中，FAMGA 面临全面制裁，数据滥用是核心。2018 年至今，FAMGA 作为全球五大科技巨头已经站稳第一梯队，无论营收还是市值都呈现昂扬向上的状态，马太效应似乎还将不断强化。事实上，新的五大巨头在各自领域内的影响力均具备一定垄断性。但是除了微软以外，其他四家均受到过实质性的本土“反垄断”制裁。而在 2020 年 7 月，美国众议院司法委员会召开了一场围绕美国四大科技巨头公司反垄断调查的听证会，亚马逊、Facebook、苹果和谷歌全部囊括其中，新一轮“反垄断”制裁开启：**1）亚马逊的指控：**利用第三方卖家数据谋利。**2）Facebook 的指控：**主导社交媒体市场，利用收购打压竞争。**3）苹果的指控：**主导应用程序市场。**4）谷歌的指控：**窃取其他网站数据及内容。

此后四家公司 CEO 都做了相关辩护，但调查仍在继续。目前来看谷歌的形势最为严峻：2020 年 10 月 20 日美国司法部已经证实对谷歌提起一级反垄断指控（首次），指控其滥用其在在线搜索中的主导地位，扼杀竞争并伤害消费者。**值得注意的是，此次，对于四家公司的指控中均含有对于数据资产的直接、间接滥用，可见数据滥用正是垄断优势的重要构成之一，**这在美国的此前两轮反垄断浪潮中并不明显存在。

2）中国反垄断：无独有偶，2020 年为反垄断元年，滴滴事件或加速监管落地。

2020 年对于中国反垄断史而言同样意义非凡。2020 年 11 月国家市场监管总局公布了*《关于平台经济领域的反垄断指南（征求意见稿）》*。要求互联网平台不得滥用市场支配地位，以不公平的高价销售商品或者以不公平的低价购买商品，也不得限定交易，排除、限制市场竞争，或差别待遇。《反垄断指南》也标志着我国反垄断监管大幕的拉开。

需要指出的是，我国科技巨头垄断程度总体仍小于美国科技巨头垄断程度，原因或在于：中国科技产业起步晚于美国 20 年左右，行业尚未完全固化。**但从 2021 年来看，我国首轮科技反垄断监管来势汹汹、加速落地。**2021 年 2 月*《关于平台经济领域的反垄断指南》*正式发布，明确“互联网不是反垄断的法外之地”。此后，国家市场监管总局多次针对平台企业开出反垄断“罚单”，包括腾讯、阿里、美团、字节跳动、滴滴等。

图表 14　发展阶段与技术开放度对比

对比维度	海外科技巨头					本土科技巨头			
	苹果	亚马逊	微软	谷歌	Facebook	阿里巴巴	腾讯	美团	百度
营收(亿元)	18700	19570	10125	11292	4932	5097	3772	976	1074
三年营收CAGR	7%	28%	18%	22%	37%	48%	35%	96%	15%
净利润(亿元)	3911	808	3135	2396	1290	1494	933	由负转正	21
三年净利CAGR	7%	70%	30%	21%	22%	51%	31%	/	-43%
发展阶段	**成熟期**	**快速成长期**	**较快成长期**	**较快成长期**	**较快成长期**	**快速成长期**	**快速成长期**	**快速成长期**	**成熟期**
业务结构	主营智能手机、智能电脑等移动终端产品	主营在线零售等	主营操作系统、办公软件等电脑软件	主营搜索引擎、在线广告、云计算等	主营社交网络、在线广告等	主营网络零售、移动支付、云计算等	主营在线游戏、在线视频、移动支付、云计算等	主营餐饮、外卖、旅游民宿等	主营搜索引擎、在线广告等
技术及业务生态	软硬一体化的封闭生态，始终把握对软件和硬件的控制，并视其为护城河	兼具封闭的大零售生态，以及开放的AWS云基础设施平台	封闭的软件生态体系，曾高举知识产权大旗反对 Linux 等开源模式，但当前开始部分转向开源	典型开放生态模式，手机硬件/应用商店/操作系统/PC浏览器均开放生态	封闭社交平台与第三方开发者合作时强调会可控制性，先后封杀 Snapchat、Wonder 等	对部分合作伙伴开放应用场景及数据，目前至少有73款开源产品	社交产品生态较封闭，如微信入口多开放给腾讯系或者相关公司，封杀过拼多多/钉钉	产品生态较封闭，支付优先采用美团月付和银行卡，构建全栈技术体系，覆盖前端、后台、系统、算法等	拥有内容开源的百家号等产品，新开发的 Apollo平台技术开源，合作对象广泛
技术开放度	**低**	**一般**	**一般**	**高**	**低**	**较高**	**较高**	**一般**	**较高**

资料来源：: wind，公司年报，华西证券研究所：备注：数据截取自 2019 年

我们认为，近期发生滴滴事件和斗鱼虎牙合并被否事件，充分反映了顶层监管的反垄断意志。尤其是滴滴事件，突出反映了互联网平台已形成“双重垄断”这一事实。**所谓“双重垄断”，即表面是在某一商业领域形成业务垄断，实质是对某一领域的个人/企业/甚至政府单位形成数据垄断和闭环。**

关于蚂蚁（阿里）和腾讯在支付领域的数据闭环问题，我们此前已经在相关报告中作了多次探讨，在此不做赘述。现以滴滴为例，分析其掌握的数据资产价值以及潜在隐患。

第一类数据资产：导航场景数据。此与特斯拉收集的数据有相似之处，主要涉及基础交通地理信息数据以及交通态势数据。当然考虑到其与特斯拉在自动驾驶能力方面的差异，所需数据的密度和精细度略低，但基本要素也都囊括其中。

第二类数据资产：个人行程数据。主要包括其 APP 违反规定收集的大量个人隐私数据，这也是目前官方表述的违规行为。事实上，出行场景涉及的要素极多，包括但不限于个人住处、主要联络人住所、工作单位、娱乐场所等，一旦出现非法流通情况，将可能对个人的生命、财产安全构成巨大威胁。

第三类数据资产：聚合后的数据。基于以上两类数据，还可以进一步聚合出更为高阶的数据，从而描绘区域经济、社会活动的现状。例如交通态势数据、区域人口聚集程度、区域经济活动时间规律等。随着数据的持续沉淀和二次分析，甚至可以得出特定城市或整个经济体的运行态势画像，巨大的数据可能性孕育巨大的安全隐患。

目前来看，国内科技巨头对于这类数据资产的使用主要还是为了寻求商业利益，如群众普遍反映的“大数据杀熟”。但如果延伸思考，数据滥用对于个人人身、财产安全，乃至对于整个国家安全的威胁，确实是更为重大的隐患，因此此番监管层重拳出击，全面审查也在情理之中。

我们认为，中美两国政府均在 2020 年前后开始整顿科技巨头并非巧合，背后的共性就是对数据资产的主权保卫与博弈。近年来，互联网和移动终端的蓬勃发展，带来便利的同时，也导致几乎所有数字化信息都能以某种形式被记录。而科技巨头，尤其是互联网平台巨头，又全力以赴地收集这些数据记录，并通过清洗、聚合、深度学习的方式对其进行二次开发，形成宝贵的数据资产。**对于主权国家而言，这些数据资产的战略意义重大。一方面，必须切实保护好本国经济体核心数据资产；另一方面，部分国家正在试图从各个方面获取他国数据。**

因此，数据资产绝不仅仅是一个商业问题，更是涉及主权安全/战略的问题，**预计未来数据反垄断立法和监管都将不断推进，对于监管机构的赋能输出将成为重要的潜在新增量。**从这个角度来看，网安产业显然也是数据新基建的重要构成。

5. 投资建议：谁最受益？格局如何？

基于产业视角，我们将安全厂商分类并梳理受益的核心逻辑如下：

1） 全能型厂商：超长产品线 + 高壁垒，整体性受益本次事件/政策红利。

全能型安全厂商指具备齐全安全产品线的厂商，至少在两到三个领域跻身市占率第一梯队，包括奇安信、深信服、启明星辰、绿盟科技、天融信五家。该类厂商的特点是具备较为全面的安全防护能力，能够以自身产品对客户进行解决方案层面的构建，满足客户的整体安全需求。

高技术壁垒是核心：多元化的核心能力包括网关能力、全面攻防能力、态势感知能力，需要围绕用户具体需求进行长期高投入。高技术能力的背后则是高研发的支撑，财务数据来看 2020 年五家上市的全能型厂商的研发投入基本位列行业前五，其中奇安信高举高打战略下研发亦是其重要投入，利润端尚未兑现，但未来业绩弹性巨大。

2） 专精型厂商：细分领域呈现竞争优势，局部性受益本次事件/政策红利。

专精型厂商指其他细分安全领域的龙头，多为深耕单一领域多年的单项冠军，包括但不限于安恒信息、卫士通、格尔软件、信安世纪、山石网科、中孚信息等。该类厂商的特点在于，在特定细分领域往往有明确的优势，但是其在通用安全产品层面(如防火墙、入侵检测、SOC、数据安全)竞争实力较弱，且没有明确的向此方向扩张的预期。

但与此同时，也需要指出其在技术含量和技术壁垒相较于全能型厂商仍有差距，业务的拓展受到较大限制，未来发展很大程度上取决于该细分领域的景气度，目前看云大物工移等新兴安全领域（龙头如安恒信息）机遇较大。

3） 审查型厂商：政策驱动特点鲜明，或是本次事件/政策红利的最大预期差。

网络空间治理近年受到高度关注，该产业下游往往为政法系统单位，在关键技术、产品、标准和渠道方面具有相对明确的进入门槛，产业竞争格局稳定，新进入者少。此外，网络空间治理涉及到一些大数据的能力和实施经验，这也构成了产业的壁垒。**该细分领域内主要参与者包括美亚柏科、中新赛克、迪普科技、恒为科技等，**近年来业绩普遍维持高增速。这一赛道的增长受政策驱动特征明显，其下游客户在需求逻

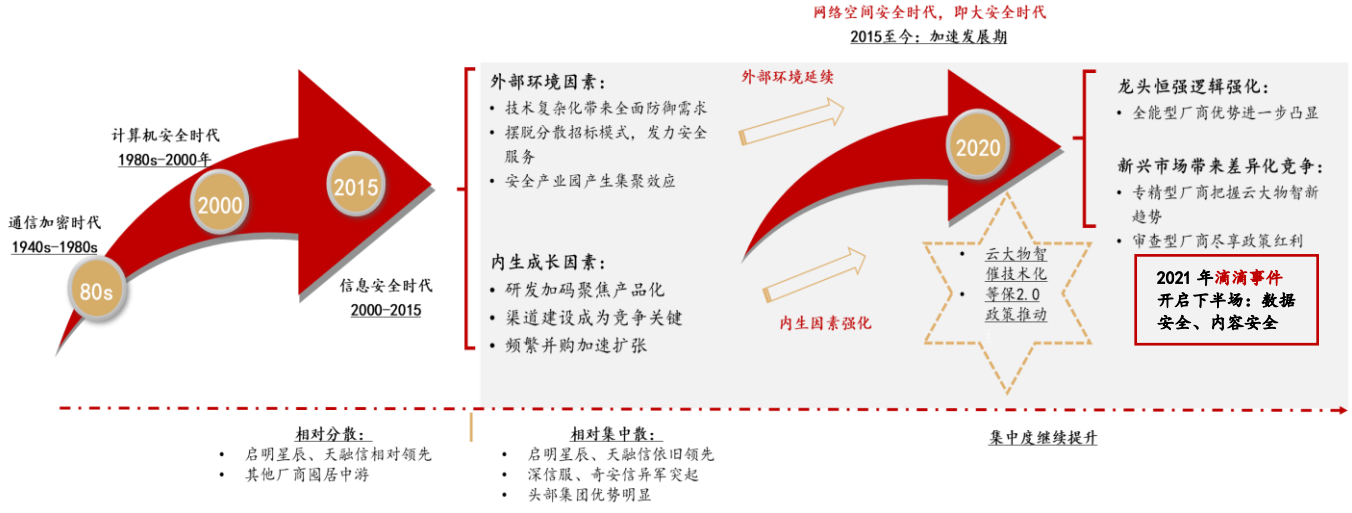
辑层面和其他三类厂商有明显不同，该细分领域下游具有鲜明的网络执法属性，业绩会受到相应政策、落地节奏、更新换代的显著影响。

赛道不同于其他网安厂商，政策特点造就一定程度的“错位竞争”。

1）美亚柏科：所在审查赛道为政府（公安等）大数据，当前仍是蓝海，政策红利持续释放。信息化一直是公安能力升级的重点，十九大以来公安部党委始终坚持改革强警、科技兴警，把大数据智能化建设作为科技兴警的重要抓手、上升为公安部党委的一项战略工程。近年来政策不断推行，而公安大数据的建设成为屡次被重点强调的核心，当前仍是建设高峰期。美亚柏科是传统网络空间安全专家，以电子取证聚焦在公安领域，尽享政策红利。随着产品应用逐步深入，公司开始利用优势积累，逐步延展产品线，在（公安）大数据审查与治理领域持续发力，龙头优势凸显。

2）中新赛克：所在的审查赛道为网络可视化，作为中央网络安全和信息化领导小组的技术支撑，赛道景气向好。2014 年 2 月 27 日，中央网络安全和信息化领导小组正式成立，标志着网络安全与信息化已经上升至国家战略，网络可视化（审查）赛道景气开启上行周期。中新赛克针对政府及公安部门等主要客户群体需求，不断进行产品研发与展业，近年来持续专注于大容量智能网卡及分流设备、无线增值业务、宽带增值业务的研发和市场拓展，为政府部门、运营商和行业用户提供成熟的通信安全保障解决方案和一站式的服务。

图表 15　网安厂商产业趋势



资料来源：华西证券研究所

投资建议：横向比较而言，坚定看好全能型厂商中的双龙头**奇安信 + 深信服**，同时大数据安全专精厂商**安恒信息**以及安全审查赛道的**美亚柏科**明确受益。

6. 风险提示

网安行业政策推进不及预期，云/态势感知等创新业务进展不及预期。

分析师与研究助理简介

刘泽晶（首席分析师）：2014-2015年新财富计算机行业团队第三、第五名，水晶球第三名，10年证券从业经验。

刘忠腾（分析师）：计算机+金融复合背景，3年IT产业+3年证券研究从业经验，深耕云计算和信创产业。

孔文彬（分析师）：金融学硕士，3年证券研究经验，主要覆盖人工智能、金融IT、网络安全研究方向。

分析师承诺

作者具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，保证报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

评级说明

公司评级标准	投资评级	说明
以报告发布日后的6个月内公司股价相对上证指数的涨跌幅为基准。	买入	分析师预测在此期间股价相对强于上证指数达到或超过15%
	增持	分析师预测在此期间股价相对强于上证指数在5%—15%之间
	中性	分析师预测在此期间股价相对上证指数在-5%—5%之间
	减持	分析师预测在此期间股价相对弱于上证指数5%—15%之间
	卖出	分析师预测在此期间股价相对弱于上证指数达到或超过15%
行业评级标准		
以报告发布日后的6个月内行业指数的涨跌幅为基准。	推荐	分析师预测在此期间行业指数相对强于上证指数达到或超过10%
	中性	分析师预测在此期间行业指数相对上证指数在-10%—10%之间
	回避	分析师预测在此期间行业指数相对弱于上证指数达到或超过10%

华西证券研究所：

地址：北京市西城区太平桥大街丰汇园11号丰汇时代大厦南座5层

网址：http://www.hx168.com.cn/hxzq/hxindex.html

华西证券免责声明

华西证券股份有限公司（以下简称“本公司”）具备证券投资咨询业务资格。本报告仅供本公司签约客户使用。本公司不会因接收人收到或者经由其他渠道转发收到本报告而直接视其为本公司客户。

本报告基于本公司研究所及其研究人员认为的已经公开的资料或者研究人员的实地调研资料，但本公司对该等信息的准确性、完整性或可靠性不作任何保证。本报告所载资料、意见以及推测仅于本报告发布当日的判断，且这种判断受到研究方法、研究依据等多方面的制约。在不同时期，本公司可发出与本报告所载资料、意见及预测不一致的报告。本公司不保证本报告所含信息始终保持在最新状态。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，投资者需自行关注相应更新或修改。

在任何情况下，本报告仅提供给签约客户参考使用，任何信息或所表述的意见绝不构成对任何人的投资建议。市场有风险，投资需谨慎。投资者不应将本报告视为做出投资决策的惟一参考因素，亦不应认为本报告可以取代自己的判断。在任何情况下，本报告均未考虑到个别客户的特殊投资目标、财务状况或需求，不能作为客户进行客户买卖、认购证券或者其他金融工具的保证或邀请。在任何情况下，本公司、本公司员工或者其他关联方均不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告而导致的任何可能损失负有任何责任。投资者因使用本公司研究报告做出的任何投资决策均是独立行为，与本公司、本公司员工及其他关联方无关。

本公司建立起信息隔离墙制度、跨墙制度来规范管理跨部门、跨关联机构之间的信息流动。务请投资者注意，在法律许可的前提下，本公司及其所属关联机构可能会持有报告中提到的公司所发行的证券或期权并进行证券或期权交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。在法律许可的前提下，本公司的董事、高级职员或员工可能担任本报告所提到的公司的董事。