证券研究报告

行业报告 | 行业深度研究

2021年08月18日

计算机

数据安全：固基修道，履方致远

作者：

分析师 缪欣君 SAC执业证书编号：S1110517080003

天风证券

[综合金融服务专家]

行业评级：强于大市（维持评级）

上次评级：强于大市

摘要

1. 我们基于数据的生命周期和《网络安全等级保护基本要求》中的安全通用技术要求，分别整理了数据安全**产品图谱和行业图谱**。此外，**数据安全治理、身份与访问管理（“零信任”体系）、隐私计算、云数据安全（SASE）**等产业与数据安全息息相关，**或成为未来数据安全产业的重要组成部分**。

2. 数据安全发展受到**监管**和**内生需求**双重因素的驱动。监管层面，**金融、水利、交通、教育、政府、电信与互联网行业**为数据安全监管较为严格的行业，**数据备份、数据分级分类、数据安全风险评估和审计**是监管最为看重的四个子领域；内生需求层面，**长期来看中国数据安全市场存在千亿市场空间**。

3. 我国数据安全市场规模预计将在2023年预计达到**97.5亿**，在整体网络安全市场占比达到**12.1%，核心客户购买实力雄厚，可贡献约40亿收入**。未来**政府、金融、医疗卫生以及能源行业**在数据安全领域的投入有望进一步打开**1至3倍的成长空间**，整体数据安全领域仍有**近1倍的弹性增长**潜力空间。

摘要

4. 六大**基础网络安全领域**，上市公司**优势产品有一定差异化**，其中安恒信息专精于应用安全、安全管理及数据安全市场，奇安信领衔终端安全与安全管理市场。**新兴赛道领域**，头部公司正加强在**云安全、车联网安全、工控安全、隐私计算和零信任**等技术与应用场景的布局。

5. 数据安全**产品布局**方面，安华金和、安恒信息、启明星辰、天融信已建立较为完整的数据安全产品线，且多家公司在**数据脱敏、数据库安全、数据泄露防护、隐私计算等**细分领域上有各自重点布局。

6. 未来上市公司在数据安全方面的发展主要有**优化完善数据安全产品线与解决方案、结合前沿技术推进传统安全产品转型升级、兼顾数据安全与数据流动、融合零信任理念、完善场景化方案**五个方向。

摘要

风险提示：1、行业监管政策发生重大调整；2、宏观经济不景气，下游客户采购需求下降导致上游产品研发投入缓于预期；3、产业核心技术发生重大调整，现有产品结构和解决方案不再具有优势；4、市场规模测算中的假设存在一定的主观推断

重点标的推荐

股票	股票	收盘价	投资	EPS(元)				P/E			
代码	名称	2021-08-17	评级	2020A	2021E	2022E	2023E	2020A	2021E	2022E	2023E
688023.SH	安恒信息	299.00	增持	1.81	2.73	4.07	7.92	165.19	109.52	73.46	37.75
300454.SZ	深信服	260.00	增持	1.96	2.42	3.15	4.13	132.65	107.44	82.54	62.95
300369.SZ	绿盟科技	19.90	买入	0.38	0.53	0.71	0.92	52.37	37.55	28.03	21.63
002439.SZ	启明星辰	30.40	买入	0.86	1.06	1.31	1.62	35.35	28.68	23.21	18.77
688561.SH	奇安信	93.65	买入	-0.49	-0.07	0.84	1.63	-191.12	-1337.86	111.49	57.45

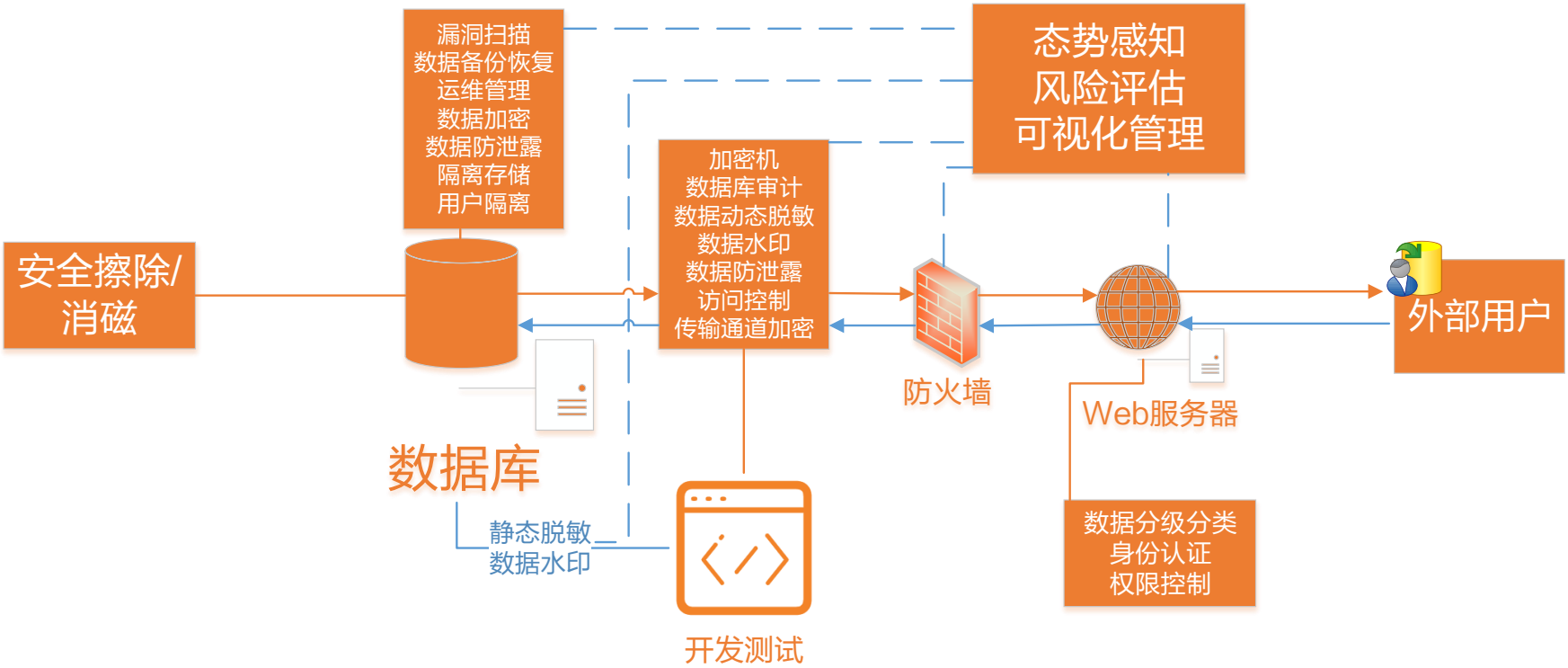
资料来源：Wind、天风证券研究所

目录

1
数据安全行业图谱

1.1 数据安全与数据全生命流程

根据《GB/T37988-2019信息安全技术 数据安全能力成熟度模型》国家标准，数据的生命周期分为采集、传输、存储、处理、交换和销毁六个阶段，在各个阶段对于数据安全的核心技术能力诉求如下图所示：



资料来源：中安威士官网、闪捷信息官网、安华金和官网、安恒信息官网、中安云科官网、深信服官网、《数据安全白皮书》（华为、工信安全）、天风证券研究所

1.2 数据安全行业与等保2.0

2019年公安部牵头发布《网络安全等级保护基本要求》（下称“要求”），其中所明确的网络安全等级保护制度已成为我国网络安全基本制度体系的通用标准，是等保2.0体系的重要标准之一。数据安全作为重要要素在要求的各个子项目中被多次强调，基于《网络安全等级保护基本要求》中的安全通用技术要求，我们梳理了以下数据安全行业图谱。

资料来源：数说安全公众号、安全牛公众号、相关公司官网、天风证券研究所

1.3 泛数据安全产业

除传统围绕数据的生命周期，沿着数据的采集、传输、交换、存储、处理与销毁流程直接与数据或者数据库相关的产品外，我们认为安全领域还有一些产业与数据安全息息相关，具体包括**数据安全治理、身份与访问管理（“零信任”体系）、隐私计算、云数据安全（SASE）**等，他们为数据安全发展提供方法论和体系框架、引入新兴技术和应用场景，或成为未来数据安全产业的重要组成部分。

表：泛数据安全产业典型应用

	描述与定义
数据安全治理	指从决策层到技术层，从管理制度到工具支撑，**自上而下建立的数据安全保障体系和保护生态**，包含**国家宏观治理**和**企业组织内部微观自治**两个层面。其中企业组织内部自治旨在规范企业组织数据全生命周期处理流程，保证数据处理活动的合规性和合法性。除具体相关技术产品外，数据安全治理多以咨询服务的形式体现。
身份与访问管理	主要指访问控制，即精选出来的一系列数据访问规则，主要包含**身份验证**与**授权**两个组成部分。身份验证是用于验证给定用户是否是其所声称的身份的一种技术，而授权技术是确定用户是否可以访问数据或执行其所尝试操作的技术。
“零信任”体系	**零信任**指一组以“信任从不被隐式授予，而是必须持续评估”为前提的概念和设计思想，而**“零信任体系”**是基于零信任的一种企业资源和数据安全端到端的保护方法，包含人和非人实体的**身份标识、认证信息、访问管理、操作运维、端点管控、运行环境和互连基础设施**等内容。
隐私计算	隐私计算体系通过融合多学科技术，使得两个或多个参与方可以在不泄漏各自数据的前提下进行联合计算，在保护数据安全的同时实现多源数据跨域合作，推进数据融合价值的挖掘。目前主流的隐私计算技术路径包含**多方安全计算、联邦学习和可信计算**三大方向。
云数据安全	云数据安全可从两个层面理解：一个层面为**把用户在数据安全上需要使用到的所有的能力抽象化，以云服务的方式提供**，以最简便的方式保证用户和开发者的数据安全；另一个层面为**云内应用的数据安全**，这包括存储数据的敏感内容发现、数据流动的监控和保护、以及数据内容的安全分析等。
SASE	SASE（Secure Access Service Edge，安全访问服务边缘）是一个**基于云化部署的网络和安全组件框架**，包含了 SD-WAN、云访问安全代理（CASB）、安全的 web 网关(SWG)、零信任网络访问（ZTNA）、防火墙即服务（FWaaS）和远程浏览器隔离（RBI）等一套技术。SASE 将**身份作为安全架构的中心**，确保通常以云服务形式提供的应用程序、服务、用户和机器对云和网络资源的安全访问。

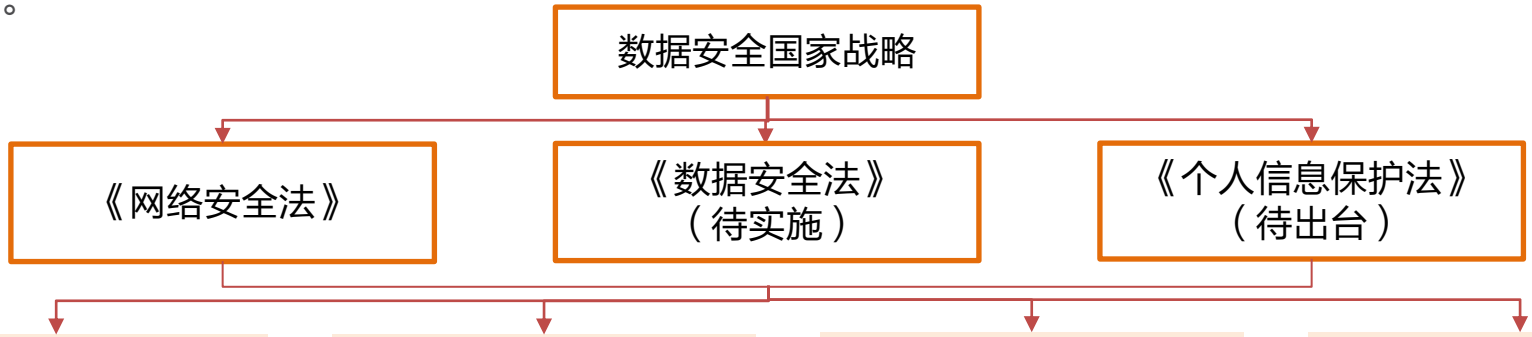
资料来源：赛迪智库、安全牛公众号、信息安全与通信保密杂志社、《腾讯隐私计算白皮书》、中国信息安全公众号、中国信通院公众号、天风证券研究所

2
数据安全行业驱动因素

2.1 外因：合规要求，稳定增长

2.1.1 数据安全监管体系框架

2015年颁布的《国家安全法》明确提出“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”，将数据安全纳入国家安全的范畴。目前我国的数据安全监管体系框架形成了以**“数据安全国家战略”**为出发点，**《网络安全法》、《数据安全法》（即将实施）、《个人信息保护法》（即将出台）为核心**，其他专项规定、行政法规、行业部门规章、以及地方性法规等为细节补充的体系框架。



其他专项规定

《信息基础设施安关键全保护条例》、《网络安全等级保护条例》、《网络安全审查办法》等

行政法规

《科学数据管理办法》、《促进大数据发展行动纲要》、《国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见》、《电信条例》等

行业部门规章

科技部、工业和信息化部、教育部、交通部、中国银保监会、中国人民银行、国家卫健委等部委负责出台对各自领域数据的管理相关的规范性文件

地方性法规

各地方政府主导制定本地大数据发展和应用相关条例，目前已有吉林、山西、海南、贵州、天津、广东等地出台了超过14个有关数据安全问题的地方性法规等文件

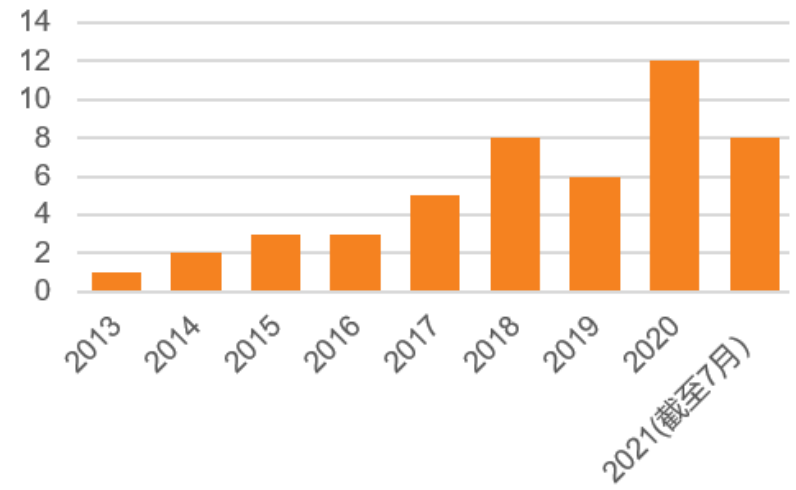
资料来源：《数据安全白皮书》（华为、工信安全）、相关政府网站、天风证券研究所

2.1 外因：合规要求，稳定增长

2.1.2 数据安全监管趋势

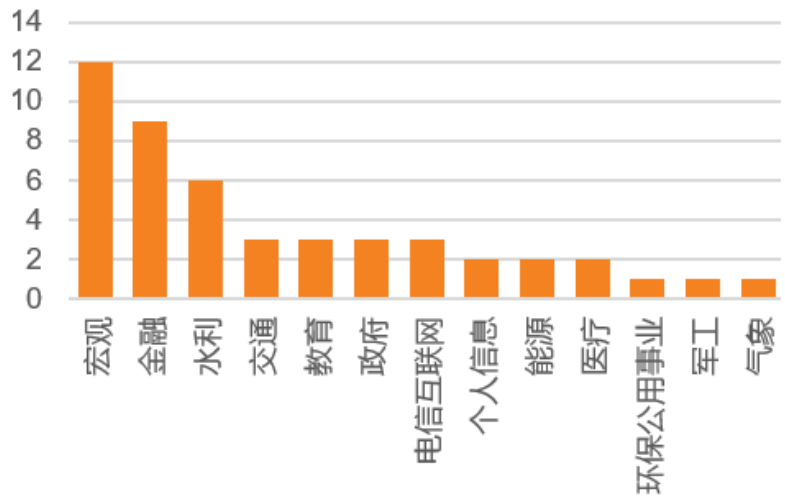
通过对中央法律法规、部委出台的文件要求、以及各行业监管部门针对各行业出台的与数据安全直接相关的政策文件的梳理与统计，可以看出监管部门对于数据安全的监管和关注程度逐年提升，且主要**由中央政府与工信部主导**（下图宏观层面政策主要由全国人大、国务院、以及工信部制定），各行业监管中**金融、水利、交通、教育、政府、电信与互联网**行业为数据安全监管较为严格的行业。

图：各年份数据安全直接相关政策发布数量



资料来源：政府网站公告、天风证券研究所

图：各行业数据安全直接相关政策发布数量



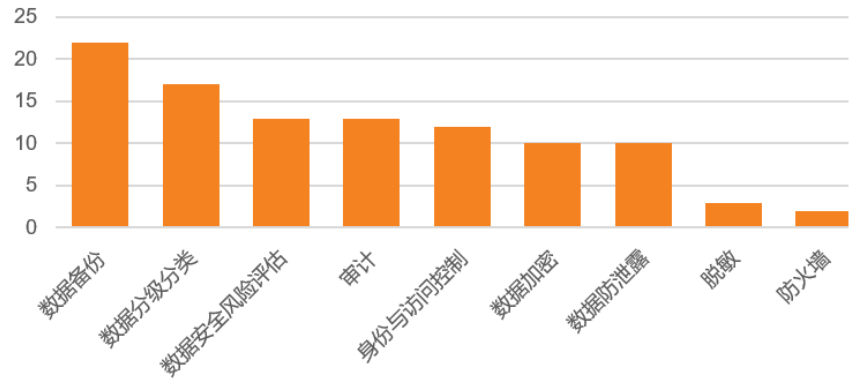
资料来源：政府网站公告、天风证券研究所

2.1 外因：合规要求，稳定增长

2.1.3 数据安全监管要求

通过对中央、部委以及各行业监管部门出台的文件中提到的与数据安全直接相关的要求进行统计，可以看出**数据备份、数据分级分类、数据安全风险评估和审计**是监管最为看重的四个子领域，此外，**身份与访问控制、数据加密、数据防泄露**也是监管重点关注的方向。此外，根据等保2.0体系下《网络安全等级保护基本要求》中的各项要求标准，参加等保2.0测评的公司需在**数据库漏洞扫描、防火墙、审计、数据加密、脱敏、水印**等产品上进行投入。

图：数据安全细分领域政策数量统计



资料来源：政府网站公告、天风证券研究所

表：等保2.0对数据安全的相关要求

等级	可能涉及的数据安全产品
一级	一级信息系统无需做等保，不需要备案，也不需要测评
二级	数据库漏洞扫描、防火墙、身份与访问控制、数据备份与恢复、数据库安全运维、数据库加密
三级	数据库漏洞扫描、防火墙、身份与访问控制、数据备份与恢复、数据库安全运维、数据库加密、数据库审计 **数据资产梳理、数据脱敏、密码、水印（大数据场景）**
四级	数据库漏洞扫描、防火墙、身份与访问控制、数据备份与恢复、数据库安全运维、数据库加密、数据库审计 数据资产梳理、数据脱敏、密码、水印（大数据场景） **态势感知**
五级	五级要求未做明确

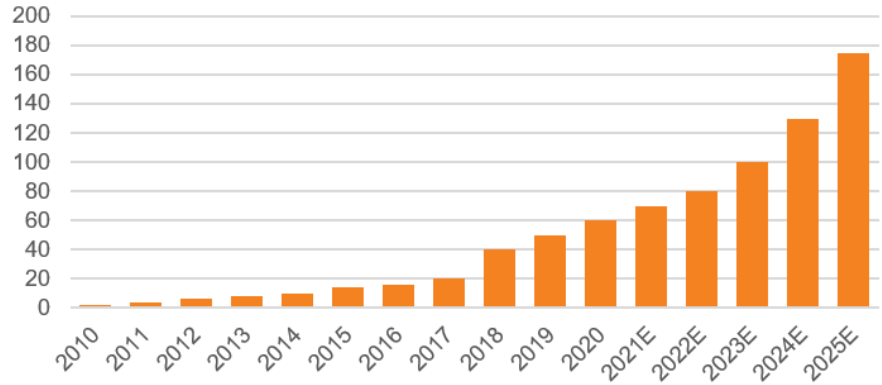
资料来源：《网络安全等级保护基本要求》、天风证券研究所

2.2 内因：内生需求，快速激活

2.2.1 数据量快速攀升，激发数据安全意识

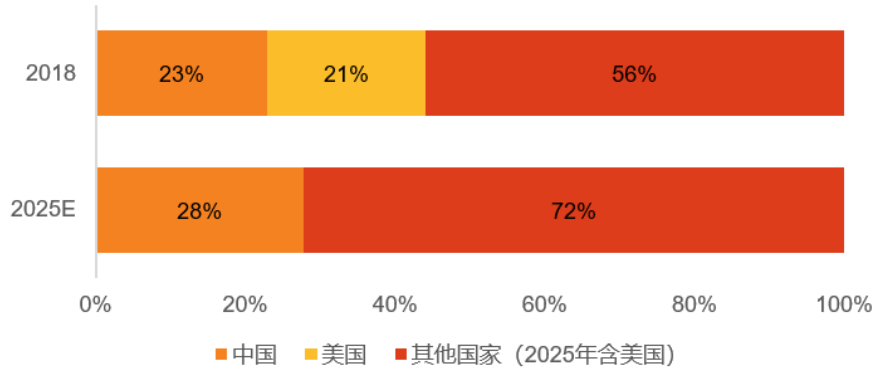
根据IDC发布的《数据时代2025》报告，到2020年，全球数据量达到了60ZB，**2025年将达到175ZB，接近2020年数据量的3倍**。同时，IDC预测**中国数据量增速最为迅猛，预计2025年将增至 48.6ZB，占全球数据圈的27.8%**，成为全球最大的数据圈（数据圈指被创建、采集或是 复制的数据集合）。随着数据量的增加，隐藏在数据背后可被挖掘的信息也逐渐丰富，无论是政府还是企业都开始意识到数据泄露可能带来的严重后果，**对数据安全的重视程度提升趋势明显**，并在积极探索**在安全可控的情况下最大化发掘数据价值**。

图：2010-2025 年全球数据量增长预测（单位：ZB）



资料来源：IDC、数据猿公众号、天风证券研究所

图：中国数据量全球占比变化



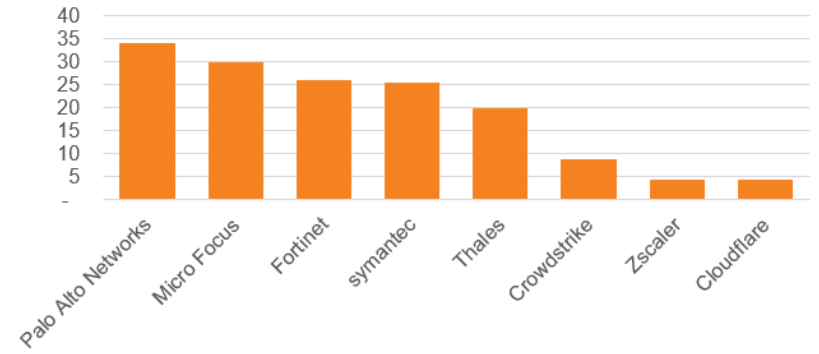
资料来源：IDC、东方财富网、前瞻产业信息研究院、《数据安全白皮书》（华为、工信安全）、天风证券研究所

2.2 内因：内生需求，快速激活

2.2.2 对标欧美，未来市场容量还有大量增长空间

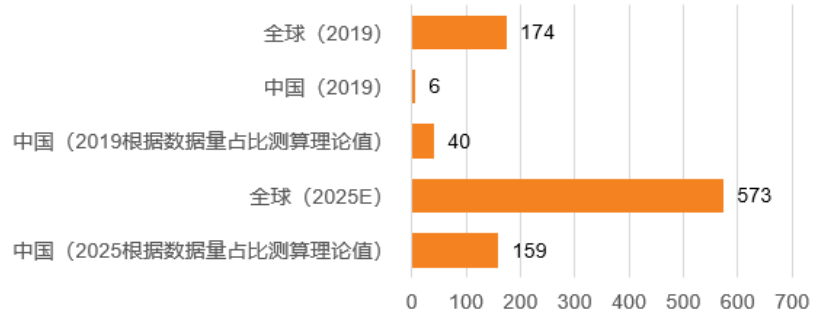
根据海外市场研究机构VMR统计，2019年全球数据安全市场规模约为173.8亿美元，且预计到2027年全球数据安全市场规模将达到572.9亿美元，年复合增长率约为17.35%。 而根据中商产业研究院统计，2019年我国数据安全市场规模仅为38亿元，**仅占全球数据安全市场规模的3.4%**，与我国整体数据量在全球23%的占比仍有较大差距，因而我们认为未来中国数据安全**市场容量仍有较大增长空间**，考虑到中国数据安全市场整体发展节奏慢于美国，**我们认为长期来看中国数据安全市场存在千亿市场空间**。

图：海外数据安全/网络安全公司 2020 年收入（单位：亿美元）



资料来源：Wind、Thales 官网、Macrotrends、Craft、天风证券研究所

图：数据安全市场规模测算（单位：亿美元）



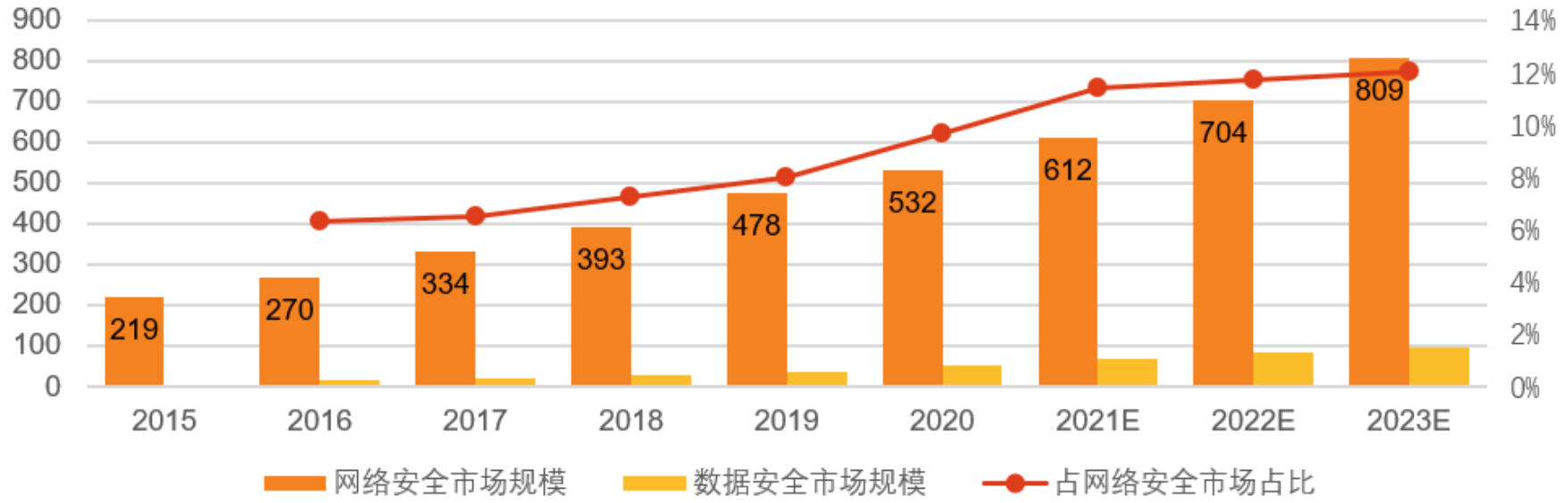
资料来源：VMR、中商产业研究院、天风证券研究所

3
细分市场规模预测

3.1 大势所趋：数据安全在网络安全市场规模占比逐年上升

根据中国网络安全产业联盟最新公布的网络安全市场规模数据，预计到2023年我国网络安全市场规模有望达到809亿，同时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%，且自2016年以来呈现连续增长态势。**

图：2015-2023 中国数据安全在网络安全市场占比（单位：亿元）

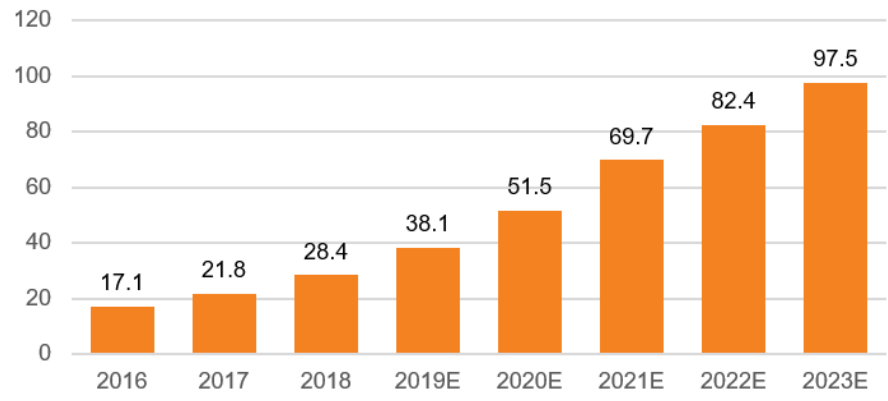


资料来源：中国网络安全产业联盟、赛迪咨询、21 财经、奇安信招股说明书、天风证券研究所

3.2 细分市场存在较大弹性增量空间

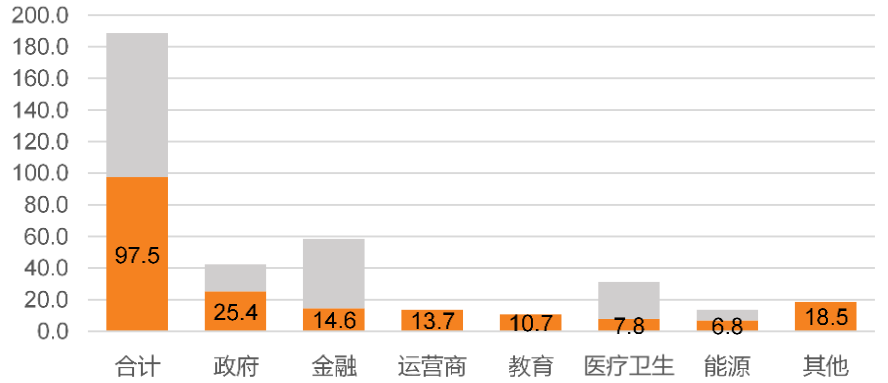
工信部在2021年7月16日发布《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》，其中提出未来三年电信等重点行业**网络安全投入占信息化投入比例达10%**，我们认为随之带动的亦包含在数据安全领域的投入。通过对现有重点行业在网络安全领域的投入占比情况进行测算，对标工信部对于10%的网络安全投入占比要求以及国际平均投入水平，我们认为未来**政府、金融、医疗卫生以及能源行业在数据安全领域的投入有望进一步打开1至3倍的成长空间，整体数据安全领域仍有近1倍的弹性增长潜力空间。**

图：2016-2023 中国数据安全市场规模（单位：亿元）



资料来源：赛迪咨询、21 财经、奇安信招股说明书、天风证券研究所

图：2023 年细分市场数据安全投入潜在增量空间测算（单位：亿元）



资料来源：工信部、Gartner、《金融行业网络安全白皮书(2020 年)》、IDC、中国电信、中商情报网、前瞻产业研究院、天风证券研究所，注：灰色部分为潜在增量市场空间

3.3 核心客户购买实力雄厚，可贡献约40亿收入

针对等保测评的核心行业和单位，我们对其在数据安全领域部分主流产品的购买力进行了测算。考虑到：1）等保2.0测评标准升级，数据安全被列为独立测评对象；2）随着数据安全监管趋严，各单位或将增大对身份鉴别、数据备份、数据库漏洞扫描、数据脱敏、数据资产梳理、态势感知等产品的购买力度；3）未来两年网络安全与数据安全整体市场增速区间约为15%-35%；我们认为**核心客户在主流数据安全产品上的投入或将进一步增加，预计每年可贡献约40亿购买力**。我们的测算过程如下：

STEP1：定义核心机构数量

核心机构	数量*	定义
科研机构	728	中央直属科研机构数量
能源	127	A 股能源行业上市公司数量
医院	1580	三甲医院数量
学校	1272	本科院校数量
电信	102	三大运营商省分公司数量
政府机构	555	中央机关及省级以下直属机构
电力	33	国网、南网省级分公司数量
金融行业	1920	金融、保险、证券公司数量
总计	**6317**	

资料来源：观研报告、Wind、卫健委、教育部、中国电信招股说明书、国家公务员网、国家电网、南方电网、中国经济网、中国证券业协会、零壹智库、天风证券研究所

*注：为方便统计，此处数量为合理预估值

×

STEP2：主流数据安全产品平均单价

主流数据安全产品	单价（万元）*
防火墙	11
身份与访问控制相关	18
数据备份与恢复	78
数据库安全运维	33
数据库加密	96
数据库漏洞扫描	15
数据库审计	23
数据脱敏	49
数据资产梳理	7
水印	19
密码	19
态势感知	52

资料来源：采招网、天风证券研究所

*注：单价为根据采招网相关订单取平均值，为降低行业特异性样本已尽可能取到各行业订单，但在具体场景下订单单价金额仍可能根据实际情况存在一定差异性

×

STEP3：每年新增采购比率假设

传统成熟产品
10%
新兴、顺应监管趋势产品
20%

资料来源：天风证券研究所

= **40.3亿元**

注：本测算假设定义中的核心机构在每年都会按照一定新增采购比率对每一类别的主流数据安全产品进行采购，实际采购过程中可能存在当年只采购部分品类的情况，但是考虑到：1）该机构年内针对特定产品可能进行多次采购，2）各品类单价差别不大；3）以及对核心机构数量的假设统计并未考虑其他省、市级分支机构，故而我们认为该假设仍具有一定参考意义。

4
网安公司数据安全产品布局

4.1 网络安全上市公司产品对比

在六大基础网络安全领域，**天融信、深信服、启明星辰**在**网络与基础架构安全领域**深耕多年，核心产品历经研发升级，在各自市场稳定占据领导地位；**安恒信息专精于应用安全、安全管理及数据安全市场；奇安信领衔终端安全与安全管理市场**；绿盟科技的IDS/IPS、WAF、ADS产品处于市场领先地位。

表：6家上市公司优势产品对比

产品所属领域	产品描述	安恒信息	深信服	天融信	奇安信	绿盟科技	启明星辰
基础安全领域							
网络与基础架构安全							
防火墙	实施访问控制策略的系统，检查流经的网络流量，拦截不符合安全策略的数据包			√			
UTM	同时将多种安全特性集成于一个硬件设备里形成的标准统一威胁管理平台		√		√		√
入侵检测与防御	检测入侵行为，根据攻击的威胁级别立即采取抵御措施			√		√	√
上网行为管理	记录、管控上网行为，管控文件外发和信息泄露		√				
VPN	虚拟专用网络，能在外网访问企业内网的资源数据		√	√			√
抗拒绝服务攻击	抵御分布式拒绝服务攻击，实现基于行为异常的攻击检测和过滤机制					√	
应用交付	用相应的网络优化/加速设备，确保用户业务应用快速、安全、可靠交付		√				
端点安全							
终端安全管理	识别终端安全风险，构建终端风险体系并对终端风险进行安全管理				√		
终端检测与响应	监视终端以检测可疑活动,并捕获可疑数据以进行安全取证及调查		√		√		
应用安全		√				√	√
web 应用防火墙	一种基础的安全保护模块，主要针对 HTTP 访问的 Web 程序保护	√				√	
数据安全		√					
数据库安全	保证数据库信息的保密性、完整性、一致性和可用性	√					
数据库审计与风险控制	专门针对数据库访问、操作行为等进行审计的系统	√					
身份与访问管理							
运维审计堡垒机	监控和记录运维人员对网络内的服务器等设备的操作行为，集中报警、审计定责	√					√
零信任	以身份为中心进行访问控制，引导安全体系架构从网络中心化走向身份中心化		√	√			
安全管理							
安全管理平台	一体化的安全管理运行的技术集成平台				√		
日志分析与审计	对日志系统记录的信息集中审计、集中分析	√					
态势感知	基于环境的、动态、整体地洞悉安全风险的能力	√			√		
威胁管理	综合多种不同的威胁处理方法，旨在威胁真正进入系统之前阻止它们				√		
城市级安全运营	为智慧城市整体运营提供 IT 运行保障	√			√		
云安全	基于云计算商业模式应用的安全软件，硬件，用户，机构，安全云平台的总称	√			√	√	
工控安全	对工业控制系统提供安全防护			√		√	√
物联网安全	对物联网（融合了计算机、通信和控制等技术的复杂系统）提供安全防护	√		√		√	√
车联网安全	应对涉及智能网联汽车的网络安全问题			√			√

资料来源：公司年报、数说安全公众号、天风证券研究所

4.1 网络安全上市公司产品对比

与此同时，**头部公司加强在新兴应用场景布局，抢占新兴赛道，目前部分市场竞争格局较为分散。**

云安全方面，安恒信息、奇安信、绿盟科技处于领先地位。**车联网安全**方面，奇安信已同车联网龙头企业高新兴达成战略合作，并携手中电互联成立合资公司。天融信参与多项行业标准、白皮书编制，已推出一系列车端安全产品。**工控安全**方面，天融信、启明星辰均有多款产品入选赛迪《中国工控安全市场发展白皮书》竞争格局中领导者行列。**隐私计算**方面，安恒信息与奇安信分别推出隐私计算产品。**“零信任”**领域，2021可信云大会上天融信、深信服成为首批零信任产品通过了零信任安全能力评估的企业。

资料来源：信息安全国家工程研究中心公众号、中国通信院CAICT公众号、各公司年报

4.2 下游客户细分行业对比

根据IDC《IDC全球网络安全支出指南，2021V1》报告，**政府、通信、金融**仍将是中国网络安全市场前三大支出行业，**占中国总体网络安全市场约五成的比例**。在我们关注的六家上市公司中，其营收占比（分行业）也呈现类似特征。其中**奇安信、天融信**主要服务政府、公检法司、军队军工行业，三者占比均达到其年度总营收的50%以上；**安恒信息**客户主要分布在政府、事业单位、金融和教育领域；**深信服**2020年营收一半以上来自政府及事业单位；**绿盟科技**相较于其他几家公司，则具有较高的运营商及金融领域客户营收占比，2020年其比重分别达到21.48%、20.61%。

表：网安公司营收占比（分行业）

	安恒信息 (2018)	深信服 (2020)	天融信 (2020)	奇安信 (2019)	绿盟科技 (2020)	启明星辰 (2007-2009 均值)
政府（及事业单位）	34.04%	54.24%	55.59%	45.48%	34.07%	39.31%
军队军工			21.05%	6.64%		
运营商	7.74%	11.45%		4.24%	21.48%	14.31%
金融	10.16%			5.17%	20.61%	11.92%
教育	9.76%			5.07%		
能源				6.49%	23.79%	
企业		34.31%	23.37%（国有）			
其他	38.30%			26.92%		34.46%

资料来源：各公司公告、招股说明书、天风证券研究所

4.3 网安公司数据安全产品布局

数据安全产品布局方面，安华金和、安恒信息、启明星辰、天融信已建立较为完整的数据安全产品线。细分领域上，数据安全厂商**安华金和**在**数据脱敏、数据库安全**方面领先国内市场，并积极布局云数据安全；绿盟科技全资子公司**亿赛通**在**数据泄露防护**市场占有率多年位居国内第一。而在隐私计算领域，除专注此赛道的翼方健数、华控清交等公司外，部分头部网络安全厂商也参与实践，以**安恒信息推出的AiLand数据安全岛、奇安信推出“数据交易沙箱”产品**为代表。

部分企业立足新兴技术领域，专注特定细分市场。易安联作为零信任安全解决方案提供商，已围绕应用访问安全共发布6款零信任系列产品；九州云腾基于认证云+应用云构建零信任网络。

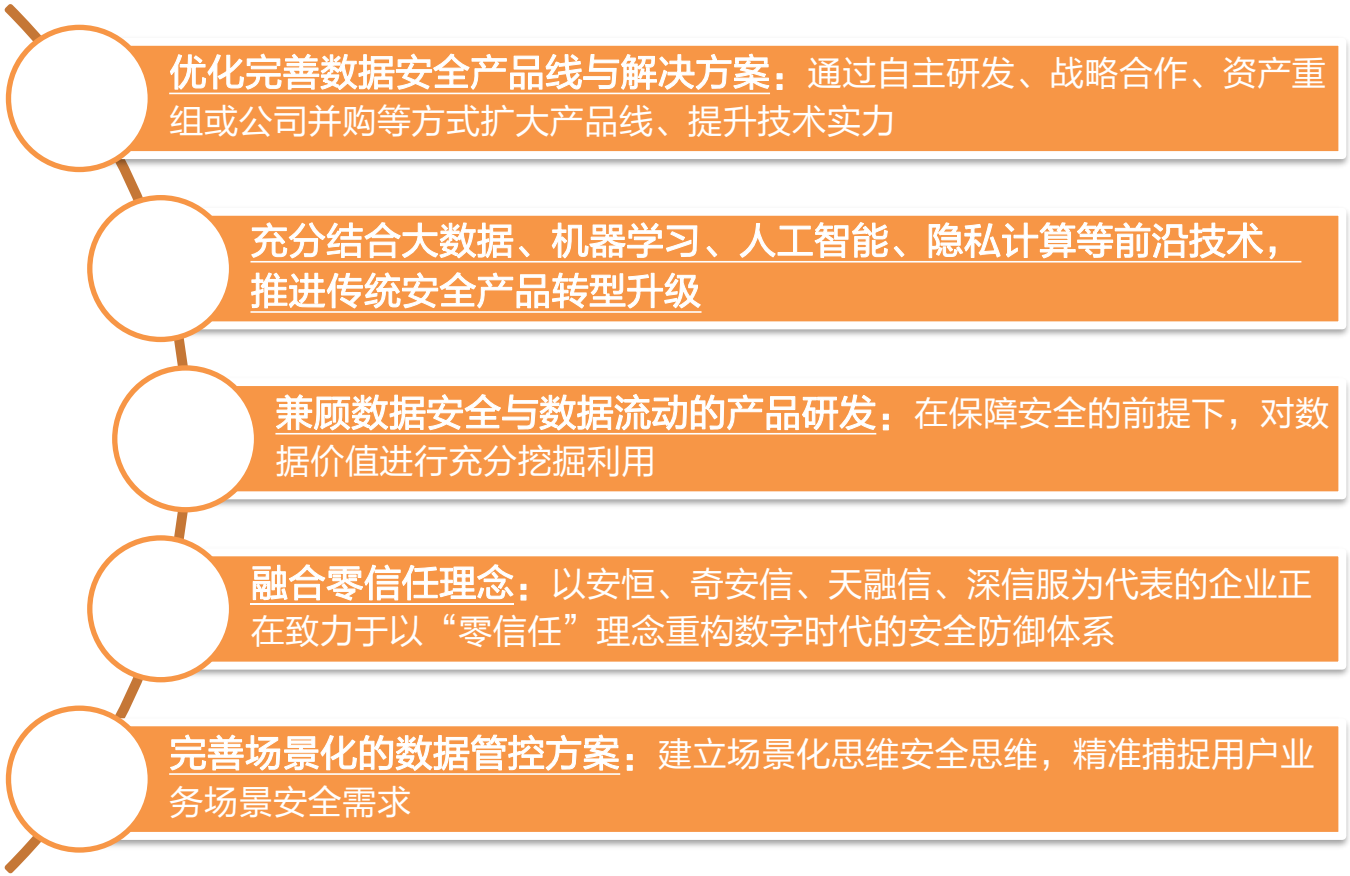
表：12 家网络安全公司数据安全产品布局

列 1	奇安信	安恒信息	绿盟科技	亿赛通	启明星辰	天融信	深信服	安华金和	明朝万达	易安联	九州云腾	科来
数据库防火墙	√	√	√	√	√	√	√	√	√			
数据库防泄露	√		√	√	√	√			√			
动态数据脱敏	√	√	√	√	√	√		√				
数据加解密		√		√				√	√			
数据水印	√	√				√		√				
数据库加解密				√				√				
数据库漏洞扫描	√	√		√	√			√				
静态数据脱敏	√	√	√	√	√	√		√	√			
数据备份和副本管理		√				√	√					
数据识别和分级分类		√	√			√	√	√	√			
数据风险评估	√	√	√		√		√	√	√			
数据库审计	√	√	√	√	√	√	√	√	√			
数据库运维管控（含堡垒机）	√	√	√		√	√	√	√				
数据库安全态势感知	√	√		√	√	√	√	√				√
数据安全管理平台		√	√	√	√	√		√	√			
“零信任”	√	√	√		√	√	√			√	√	
隐私计算	√	√										
云数据安全	√	√	√		√	√	√	√				

资料来源：各公司官网、天风证券研究所

4.4 数据安全发展五大布局方向

通过对上市公司所披露的在数据安全领域的产品和研发投入进行梳理，我们认为未来上市公司在数据安全领域的布局主要有五个方向：



4.4 数据安全发展五大布局方向

表：上市公司数据安全领域产品和研发重点投入梳理

公司名称	数据安全领域产品和研发重点投入
安恒信息	1）“赋能数据开放、激活数据价值”
	2）综合的数据安全解决方案：包含“CAPE”数据全生命周期防护体系、数据安全咨询服务体系、AiLand 数据安全岛、AiTrust 零信任解决方案、AiDSC 数据安全管控平台、EDR 与数据勒索防护等六大产品服务，全面覆盖政企单位的数据安全风险
	3）聚焦态势感知在监管、公安和金融风险监测领域的应用；助力数据共享与业务协同，提供全生命周期的监测与防护解决方案
奇安信	1）重点布局态势感知、数据隐私保护、云安全、零信任身份安全等新赛道
	2）发布数据安全开放平台和数据安全治理与保护体系建设路径图
	3）充分结合大数据、机器学习、人工智能等前沿技术：大数据隐私计算沙箱，基于 AI 对敏感文档的分级分类处理及识别源程序类型，数据可视化操作平台等
天融信	1）推出了以数据安全治理为基础、数据安全防护为核心、数据安全监管为目标的完整数据安全建设方案，在运营商、金融、政府等多个行业领域得到广泛应用
	2）通过自主研发、战略合作、资产重组或公司并购等方式扩大产品线
	3）数据安全业务收入增幅不低于 80%
启明星辰	1）传统数据安全产品升级：发布数据库动态脱敏系统，进一步满足用户业务系统实时性、高频性的数据脱敏需求
	2）聚焦云安全：构建网络安全、主机安全、应用安全、数据安全、原生安全等全方位安全闭环体系
	3）完善场景化的数据管控方案，重要的研发投向包含态势感知系统、数据安全治理平台等项目
绿盟科技	1）优化完善数据安全产品线与解决方案：发布业内首款敏感数据发现与风险评估系统、数据脱敏系统以及数据安全平台等多类新品
	2）增大投资布局：全资收购数据安全传统厂商亿赛通、投资安华金和完善在数据安全产品领域布局。、
深信服	1）人工智能、机器学习与数据安全结合：实现智能分类分级、数据流转检测和溯源等领域的技术突破
	2）与零信任理念融合：提出“以零信任理念重构终端数据安全防线”
	3）深入布局安全 SaaS 业务 SASE“云安全访问服务 Sangfor Access”，正式开始进入安全能力的云化交付时代

资料来源：各公司年报及公告、和讯网、品牌强国官网、安全牛、启明星辰公众号、深信服公众号、天风证券研究所

5
风险提示

风险提示

1. 行业监管政策发生重大调整

2. 宏观经济不景气，下游客户采购需求下降导致上游产品研发投入缓于预期

3. 产业核心技术发生重大调整，现有产品结构和解决方案不再具有优势

4. 市场规模测算中的假设存在一定的主观推断

分析师声明

本报告署名分析师在此声明：我们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，本报告所表述的所有观点均准确地反映了我们对标的证券和发行人的个人看法。我们所得报酬的任何部分不曾与，不与，也将不会与本报告中的具体投资建议或观点有直接或间接联系。

一般声明

本报告是机密的，仅供我们的客户使用，天风证券不因收件人收到本报告而视其为天风证券的客户。本报告中的信息均来源于我们认为可靠的已公开资料，但天风证券对这些信息的准确性及完整性不作任何保证。本报告中的信息、意见等均仅供客户参考，不构成所述证券买卖的出价或征价邀请或要约。该等信息、意见并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对任何人的个人推荐。客户应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专家的意见。对依据或者使用本报告所造成的一切后果，天风证券及/或其关联人员均不承担任何法律责任。

本报告所载的意见、评估及预测仅为本报告出具日的观点和判断。该等意见、评估及预测无需通知即可随时更改。过往的表现亦不应作为日后表现的预示和担保。在不同时期，天风证券可能会发出与本报告所载意见、评估及预测不一致的研究报告。

天风证券的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。天风证券没有将此意见及建议向报告所有接收者进行更新的义务。天风证券的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

特别声明

在法律许可的情况下，天风证券可能会持有本报告中提及公司所发行的证券并进行交易，也可能为这些公司提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。因此，投资者应当考虑到天风证券及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突，投资者请勿将本报告视为投资或其他决定的唯一参考依据。

投资评级声明

类别	说明	评级	体系
股票投资评级	自报告日后的6个月内，相对同期沪深300指数的涨跌幅	买入	预期股价相对收益20%以上
		增持	预期股价相对收益10%-20%
		持有	预期股价相对收益-10%-10%
		卖出	预期股价相对收益-10%以下
行业投资评级	自报告日后的6个月内，相对同期沪深300指数的涨跌幅	强于大市	预期行业指数涨幅5%以上
		中性	预期行业指数涨幅-5%-5%
		弱于大市	预期行业指数涨幅-5%以下

THANKS