

网络安全托管

作者 王艺玮

摘要 网络安全托管属于网络安全服务的典型代表，主要指将企业信息化的网络安全维护环节外包予第三方网络安全托管服务提供商（Managed Security Service Provider，MSSP）；托管安全服务供应商通过其安全运营中心（Security Operations Center，SOC）及相关服务水平协议（Service Level Agreement，SLA）为客户提供全天候入侵安全检测、威胁分析、预警情报、应急响应、快速系统恢复等网络安全产品或服务。专业人员进行安全运维及企业安全管理策略咨询等服务，网络安全托管及委托托管服务概念相对超前，安全服务供应商向客户提供一站式运营管理服务以提高企业综合安全防护；有效解决安全产品部署及运维难题；其覆盖企业IT与云资产评估、风险监测、漏洞扫描、安全监控及应急响应六大主要服务，由于中国安全即服务风险、网络安全企业人才缺口、等保政策趋严等因素将有望推动中国网络安全托管行业概念普及、市场扩容。AI技术带动网络安全托管所需技术短期效益提升，推动安全运营及托管的流程自动化、技术智能化发展，进一步降低成本分析及响应周期，提升人力分析效率，为数字化时代下安全服务和运营即服务奠定基础。

行业 属于分类:信息传播、软件和信息技术服务业/软件和信息技术服务业/信息安全服务业/信息安全服务业/信息安全服务

1. 网络安全托管行业定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络资源不中断。

网络安全托管服务（Managed Security Services，MSS），即将自己业务系统的安全运维工作外包给外部专业的安全服务提供商，自己不再承担系统的安全运维工作。网络安全托管服务是安全产品、专业安防专家团队运维及企业安全管理策略咨询的集成性服务。

2. 网络安全托管行业分类

根据服务类型分类，网络安全托管市场分为客户本地驻场托管服务、远程托管安全服务和云托管安全服务三大类。客户本地驻场托管服务是依靠本地的安全网络安全管理平台等产品进行网络安全托管服务；远程托管安全服务由网络安全托管服务提供商内部工作人员远程指导全流程操作，云托管安全服务根据云上安全风险情况提供具体托管服务。

类型名称	类型说明
客户本地驻场托管服务	客户本地驻场托管服务，依靠本地的安全网络安全管理平台等产品和驻场运维人员，实现对本地网络设备、网络安全设备流量和日志等的采集处理、深度分析和事件处置。
远程托管安全服务	远程托管安全服务，即客户选择网络安全托管服务商，由网络安全托管服务提供商直接分配公司内部工作人员远程指导网络安全服务全流程落地，全程没有指派人员进行客户跟踪、现场指导。
云托管安全服务	云托管安全服务，可以根据云上安全风险情况或在不同时间段的安全防护要求，提供云上安全产品防护策略优化服务。

3. 网络安全托管行业特征

网络安全托管行业特征表现为技术门槛高、本地化合作运维、产业集中度低的特点。网络安全托管行业属于技术密集型行业，对技术革新、人才质量要求较高。网络安全托管行业主要依靠本地产品和驻场运维人员，实现网络安全维护。网络安全托管行业竞争格局较为分散，产业集中度偏低。

技术门槛较高	网络安全托管行业属于技术密集型行业，对技术要求较高 网络安全托管行业属于技术密集型行业，对产品研发和技术创新要求较高。一方面，网络安全技术和产品的创新能力是推动企业取得竞争优势的关键因素；另一方面，不同行业、不同客户对网络安全产品的技术需求也不尽相同，承接网络安全托管的企业只有在充分了解用户需求的基础上，才能研发出匹配用户真实需求的产品和解决方案。
本地化合作运维	依靠本地产品和驻场运维人员，实现网络安全维护 网络安全托管服务为合作者提供运维能力，合作者使用专用的运维通道为用户提供代维服务，并且整个服务过程可监控，管理维护能力方面保持原有的专属资源视角和能力，一般依托本地的安全网络安全管理平台等产品产品和驻场运维人员，实现对本地网络设备、网络安全设备流量和日志等的采集处理、深度分析和事件处置。
产业集中率低	网络安全托管行业竞争格局较为分散 网络安全行业产业集中度较低，网络安全托管行业竞争格局较为分散。启明星辰、奇安信、安恒信息、深信服以及绿盟科技为中国主要的网络安全托管公司，市场份额分别为12.4%、9.8%、8.3%、7.8%以及7.7%，构成中国网络安全托管行业46.0%的市场份额，剩余市场份额被其他网络安全公司瓜分。

4. 网络安全发展历程

中国网络安全行业起步于1987年，直至2000年，行业一直处于以抗病毒为代表的系统(主机)层面单点威胁被动应对式防护阶段；在技术的推动下，中国网络安全在2003年之后迅速发展，随着相关政策的落地，互联网安全技术被引入到网络安全防护中。2014年中国网络安全和信息化领导小组成立，中国网络安全行业进入以数据为重要驱动力，以大数据、云计算和人工智能为核心技术的动态积极防御阶段，并逐步进入了高速发展的时期。

开始时间：1987 结束时间：2000 阶段：萌芽期 行业动态：1987年，国家成立信息中心信息安全处 1994年，公安部颁布《中华人民共和国计算机信息系统安全保护条例》 1995年，天融信成立 1996年，启明星辰、北信源成立 2000年，深信服成立。同年也是杀毒软件市场混战时期	行业影响/阶段特征：中国网络安全市场尚未完全形成，企业网络安全相关需求快速增长，技术变动较大，无成熟技术标准，行业竞争状况和用户特点不明确。当前阶段，行业处于以抗病毒为代表的系统(主机)层面单点威胁被动应对式防护阶段
开始时间：2001 结束时间：2012 阶段：启动期 行业动态：2003年，启明星辰推出天境分布式漏洞扫描与安全评估系统 2007年-2008年，《信息安全等级保护管理办法》和《信息安全等级保护基本要求》颁布实施 2010年，启明星辰挂牌上市 2012年，绿盟科技推出“Web应用漏洞扫描系统”；启明星辰推出万兆WAF、万兆ADM	行业影响/阶段特征：主要网络安全企业基本明确自身核心技术、管理体系和市场竞争地位，企业营收增长态势良好，行业进入快速成长期。 中国网络安全市场从信息安全转向网络安全，互联网安全技术被引入到网络安全的防护中。当前阶段，处于以防火墙(安全网关)为代表的静态综合式网络纵深防御阶段
开始时间：2014 结束时间：2022 阶段：高速发展期 行业动态：2014年，中国网络安全和信息化领导小组成立 2015年，腾讯和启明星辰达成合作；中国网络安全产业联盟成立 2016年，中国网络安全协会成立；南洋股份并购天融信、航天发展并购锐安科技；同年，《中华人民共和国网络安全法》出台 2019年，十三届全国人大常委会第十四次会议表决通过《密码法》 2021年，《中华人民共和国数据安全法》出台	行业影响/阶段特征：该阶段中国网络安全行业处于高速发展期，以机器学习、人工智能为核心，检测防御和应急响应为关键的第三代网络安全技术迅速发展当前阶段，行业处于以数据为重要驱动力，以大数据、云计算和人工智能为核心技术的动态积极防御阶段

5. 网络安全托管产业链分析

伴随着中国数字化转型，大量企业将其业务迁移至云端。由于上云企业的IT环境转变为混合云、多云的架构，其环境复杂性将大幅提高，网络安全暴露面加大，网络安全需求持续释放。网络安全托管作为一种新兴的服务类型，在政策与市场的双重激励作用下，网络安全托管行业快速发展。网络安全托管行业上游是基础硬件以及软件系统，中国基础硬件设备市场集中度较高，龙头企业主导市场，中国应用最为广泛的软件系统厂商主要为浪潮、五禾恒润等龙头企业，供应稳定。

网络安全托管行业中游为网络安全产品及托管服务提供商。安全托管服务提供商主要分布三大阵营，涵盖大型云服务商、电信运营商及领先的公共安全、大型云服务商供应链代表企业华为、阿里、电信运营商代表企业为电信，网络安全公司代表企业为奇安信、深信服等，逐渐发展成为领先的基于大数据、人工智能和信息安全技术的网络安全服务提供商。

网络安全托管行业下游为政府、金融、军工、教育等应用领域。伴随着互联网产业的快速发展，目前的网络安全产品与服务已脱从传统的互联网安全领域扩展到了云计算、大数据、物联网、5G等多个方面，网络安全托管服务为构建安全管理数字化中台提供关键技术支撑，保障行业资源安全性，在各个领域的渗透率也将不断提升。

上游环节	上游说明	上游参与方
基础硬件设备	网络安全托管行业上游包括基础硬件以及软件系统。网络安全托管行业上游包括基础硬件，如芯片、内存、存储设备、网卡等设备。中国芯片厂商数量多，竞争大，技术含量高、安全性能高的高端芯片主要依赖进口。以服务器、存储系统、交换机芯片的基础元器件技术不断进步，实现国产化。 中国基础硬件设备市场集中度较高，龙头企业主导市场，主要参与者包括东方通、新华三、捷捷网络、惠来等	北京华道恒恒科技有限公司、戴尔（中国）有限公司
基础软件系统	网络安全托管服务需搭建软件系统设备，通过提供解决方案满足客户对细分市场的需求，中国应用最为广泛的软件系统厂商主要为浪潮、五禾恒润等龙头企业，供应稳定。 软件系统，如操作系统、数据库、中间件等。中国的技术基础还比较薄弱，而在引擎、算法、规则库等基础能力上相对成熟。	浪潮集团有限公司、思科系统（中国）网络技术有限公司、北京东方通科技股份有限公司、北京五禾恒润科技有限公司

中游环节	中游说明	中游参与方
网络安全产品及托管服务提供商	网络安全托管行业中游为网络安全产品及托管服务提供商。 安全产品包含安全设备、安全服务。安全设备包括身份认证和鉴定、密码、安全审计、VPN/防火墙、入侵检测与防御、统一威胁管理等。安全服务包括安全培训服务、安全管理与检测服务、安全咨询服务等。 安全托管服务提供商主要分布三大阵营，涵盖大型云服务商、电信运营商及阿里、网络安全公司。 大型云服务商供应链代表企业为华为、阿里、电信运营商代表企业为电信，网络安全公司代表企业为奇安信、深信服等。 安全托管服务提供商专注于网络安全安全，向政府、企业用户提供新一代企业级网络安全产品和服务，已发展成为中国领先的基于大数据、人工智能和信息安全运营的网络安全托管服务提供商。	启明星辰信息技术集团股份有限公司、深信服科技股份有限公司、奇安信科技集团股份有限公司、杭州安恒信息技术有限公司、华先拓安股份有限公司、阿里巴（中国）网络技术有限公司、中国电信集团有限公司、亚信安全科技股份有限公司

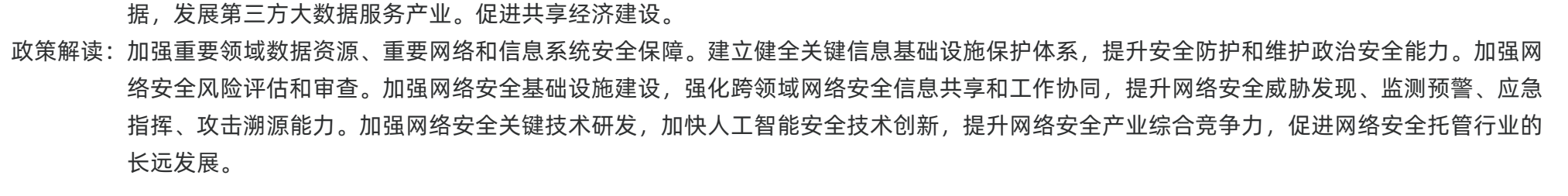
下游环节	下游说明	下游参与方
应用领域	网络安全托管行业下游为政府、金融、军工、教育等应用领域。伴随着互联网产业的快速发展，目前的网络安全产品与服务已脱从传统的互联网安全领域扩展到了云计算、大数据、物联网、5G、移动安全、车联网等多个方面，涵盖了政府机关、军队、卫生服务、教育机构、银行、能源企业、汽车企业、零售企业等服务对象。 网络安全托管服务为构建安全管理数字化中台提供关键技术支撑，保障行业资源安全性。有力推动着行业进一步扩展着物联网、AI等高新技术的结合。中国可管理安全业务未来市场将有望进一步拓展，在各个领域的渗透率也将不断提升。	新东方教育科技集团有限公司、国家电网有限公司、华为技术有限公司、博世（中国）投资有限公司

6. 网络安全行业规模

在云计算、大数据、物联网及人工智能技术驱动下，中国企业数字化程度逐渐提升，科技进步引发了新的网络安全问题：攻击者更易借助无服务器计算隐藏活动踪迹逃避网络威胁；新的网络攻击方式针对大数据、5G、物联网不断革新，对网络安全行业提出新要求。数据的产生流通和应用更加普遍化和常态化，使网络安全防范更加复杂，对第三方网络安全托管服务供应商提出更高的要求。企业信息安全防御关口逐步前移，从被动防御转向主动防御；同时，安全即服务风险持续推动下，中国网络安全商业模式实现从“产品”到“中国网络安全托管的产品、服务”模式转型。

2017年起，中国网络安全托管市场规模为90.2亿元，2017-2021年复合增长率为25.3%。随着中国IT支出规模逐步提升，托管网络安全服务行业作为网络安全服务行业的典型代表，未来整体安全市场发展前景较大。2021年，《网络安全法》以及相关法律法规的颁布直接推动了整体网络安全市场的快速发展，在政策利好、积压需求爆发等因素的影响下，中国网络安全托管行业市场规模实现了高速增长。未来，伴随企业上云节奏的进一步加快，远程托管将成为该市场实现长期高速增长的重要驱动力，中国网络安全托管市场规模保持在25%左右，预计2026年中国网络安全托管行业市场规模为616.7亿元，预计2021-2026年复合增长率为22.7%。

中国网络安全托管行业市场规模（亿元），2017-2026E



中国网络安全托管行业市场规模-中国网络安全行业市场规模-中国网络安全服务市场占比

亚信安全招股书，IDC

7. 网络安全托管政策梳理

政策名称：《关于加快推进制造业数字化转型工作的通知》 颁布主体：国务院 生效日期：2020-09 影响：6 政策性质：指导性政策
政策内容：建设态势感知平台、新型网络攻击方式针对大数据、5G、物联网不断革新，对网络安全行业提出新要求。数据的产生流通和应用更加普遍化和常态化，使网络安全防范更加复杂，对第三方网络安全托管服务供应商提出更高的要求。企业信息安全防御关口逐步前移，从被动防御转向主动防御；同时，安全即服务风险持续推动下，中国网络安全商业模式实现从“产品”到“中国网络安全托管的产品、服务”模式转型。

政策解读：推动新一代信息技术与制造业深度融合，打造数字经济新优势决策部署，促进国有企业数字化转型、网络化、智能化发展，着力落实数字化转型基础：建设基础数字技术平台、建立系统化管理体系、构建数据治理体系，提升网络安全防护水平，促进网络安全托管行业技术进一步发展。

政策名称：《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》 颁布主体：全国人大 生效日期：2021-03 影响：5 政策性质：指导性政策
政策内容：培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业，提升通信设备、核心电子元器件、关键软件等产业水平。构建基于5G的应用场景和产业生态，在智能交通、智慧物流、智慧医疗等重点领域开展试点示范，鼓励企业开放数据、电、网、云、数据，发展第三方大数据服务产业，促进共享经济健康发展。

政策解读：加强重要领域数据资源、重要网络和信息系统安全保障。建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。加强网络安全风险评估和审查。加强网络安全基础设施运营，强化网络安全信息资源共享和工作协同，提升网络安全威胁发现、监测预警、应急处置、攻击溯源能力。加强网络安全关键技术研发，加快人工智能安全技术创新，提升网络安全产业综合竞争力，促进网络安全托管行业的长远发展。

政策名称：《新型数据中心发展三年行动计划（2021-2023年）》 颁布主体：工业和信息化部 生效日期：2021-07 影响：8 政策性质：鼓励性政策
政策内容：强化数据资源管理。加强数据中心承载数据全生命周期安全管理机制建设，落实行业数据分类分级、重要数据保护、安全共享、审计法规、数据治理成熟度评估等基础制度和标准规范，强化企业数据安全主体责任落实，加强多方安全计算等数据安全关键技术创新突破与推广应用。

政策解读：推动提升网络安全保障能力。建设安全态势感知、流量分析、威胁处置等网络安全手段能力，面向数据中心底座设施和关键设备加强安全检测，防范化解多层次安全风险隐患。强化大型数据中心安全协同，构建边缘侧和云侧联动的安全威胁分析能力。

政策名称：《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）》 颁布主体：工信部 生效日期：2021-07 影响：7 政策性质：指导性政策
政策内容：加快建设创新能力、产业结构优、供给质量高、需求释放足、产融合作深、人才队伍专的健康有序产业发展生态，推动网络安全产业实现技术先进、产业发达的高质量发展目标，不断提升国家网络安全保障能力。

政策解读：加快建设创新能力、产业结构优、供给质量高、需求释放足、产融合作深、人才队伍专的健康有序产业发展生态，推动网络安全产业实现技术先进、产业发达的高质量发展目标，不断提升国家网络安全保障能力，为网络安全托管服务行业的发展打下坚实基础。

8. 网络安全托管竞争格局

中国网络安全托管行业的龙头企业是深信服、奇安信，2021年，网络安全营收规模为114,399.4万元，毛利率为58.9%；奇安信的营收规模为65,927.7万元，毛利率为59.3%；天融信的营收规模为87,995.3万元，毛利率为67.2%，达到行业前三。三者凭借其全面的安全性能力、优秀的差异化服务能力以及行业领先的品牌影响力，进入中国网络安全托管行业第一梯队。

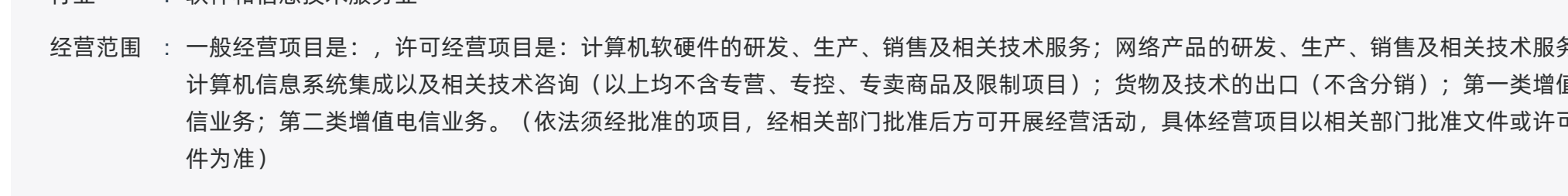
卫士通、启明星辰、安恒信息等，在中国网络安全行业多年的发展，建成全链条以防为核心的技术能力体系，从漏洞挖掘与利用，到攻击检测与响应，再到全网攻击态势感知等环节，进入行业第二梯队。

第三梯队为中小型网络安全托管企业，主要特点为产品之间差异化较小，服务出现一定的同质性，所以以价格竞争或技术竞争为主，构成行业第三梯队。中国网络安全行业正处于高速发展期，网络安全政策法规持续完善，网络安全市场规范性逐步提升，政企客户在网络安全产品和服务上的投入也将增长；随着数字经济的发展，物联网建设的逐步推进，网络安全作为数字经济发展的必要保障，其投入将持续增加。网络安全市场快速增长，市场机遇也将带来较多参与，竞争相对激烈。随着网络安全行业的快速发展，会吸引更多的竞争者进军政企网络安全领域。

X轴名称：毛利率 **单位**：百分比

Y轴名称：研发投入 **单位**：亿元

α轴名称：营收规模 **单位**：万元



横坐标：毛利率（百分比）；纵坐标：研发投入（亿元）；气泡大小：营收规模（万元）。选取这3个维度的原因是毛利率，代表公司盈利水平；研发投入，代表公司在网络安全层面研发投入水平；营收规模，代表公司承接网络安全托管服务的能力

上市公司对比

股票代码	上市公司	总市值	营收规模	同比增长(%)	毛利率(%)
688023	杭州安恒信息技术股份有限公司	108.492亿元	53,462.45万元	15.78	53.12
688561	奇安信科技集团股份有限公司	343.84亿元	65,927.71万元	44.52	59.25
300454	深信服科技股份有限公司	434.37亿元	114,399.37万元	4.76	58.86
002439	启明星辰信息技术股份有限公司	181.39亿元	56,404.66万元	11.58	68.51
300369	绿盟科技集团股份有限公司	74.75亿元	32,655.36万元	34.64	63.32
002212	天融信科技股份有限公司	124.23亿元	87,995.26万元	24.77	67.17
300386	飞天诚信科技股份有限公司	47.11亿元	39,799.33万元	25.70	33.55
002268	成都卫士通信息产业股份有限公司	257.91亿元	63,076.35万元	123.07	34.69

9. 网络安全托管代表企业分析

深信服科技股份有限公司【300454】

注册资本：41565.1628万人民币
企业总部：深圳市
行业：软件和信息技术服务业
经营范围：一般经营项目是：许可经营项目是：计算机软硬件的研发、生产、销售及相关技术服务；网络产品的研发、生产、销售及相关技术服务；计算机系统集成及相关技术咨询（以上均不含专营、专控、专卖商品及限制类项目）；货物及技术的出口（不含分销）；第一类增值电信业务；第二类增值电信业务。（依法须经批准的项目，经相关部门批准后方可开展经营活动，具体经营项目以相关部门批准文件或许可证件为准）
股票类型：A股
品牌名称：深信服科技股份有限公司
：

深信服科技股份有限公司财务数据分析

财务指标	2017	2018	2019	2020	2021	2022(Q1)	2022(Q2)
销售现金流/营业收入	1.16	1.17	1.13	1.19			
营业收入同比增长(%)	41.2805	30.4139	42.3467	18.9219	24.669	4.761	8.857
归属净利润同比增长(%)	122.6749	5.1884	25.7965	6.6512			
每股经营现金流(元)	2.13	2.3398	2.7998	3.1847	2.385	-1.668	-1.293
毛利率(%)	75.4955	73.3234	72.1855	69.9845			60.67
营业收入滚动环比增长(%)	41.5652	31.3765	45.8641	47.5726			
经营现金流/营业收入	2.13	2.3398	2.7998	3.1847	2.385	-1.668	-1.293
净利率(%)	23.1962	18.7094	16.5341	14.8281	4.0097	-45.258	-24.496
存货周转天数(天)	41.3048	45.1133	46.3696	41.8488	41	68	61
营业收入收入(元)	24.724亿	32.244亿	45.904亿	54.584亿	68.054亿	11.444亿	28.154亿

深信服科技股份有限公司竞争优势

全面的安全性——深信服拥有“SD-WAN+最全安全栈”，是领先的SASE提供商1深信服SD-WAN技术全面，兼具安全和广域网能力；深信服零信任组件技术路径创新、产品落地情况良好；竞争优势明显深信服SASE在安全和云上深洞察，各个组件几乎无短板、具备多维优势

SD-WAN产品云化特征——“云+网+端”，好的产品三者缺一不可，深信服具有这三个方面的能力。目前市场上的厂商大多比较片面，仅是各自擅长的领域有优势。在SD-WAN当前主流厂商中，深信服的竞争优势体现在于安全性能的全面和SD-WAN产品云化特征。

重视研发，持续创新——公司坚持持续的技术创新，重视研发投入，连续6年研发投入费用占营业收入的比重超过20%。

广泛渠道基础带来的经营优势——深信服坚持全国化的战略，在经过十多年的渠道体系建设，积累了大量优质的合作伙伴，渠道网络相对完善且覆盖广泛，逐步形成了现有的规模效应，为大量产品的推广和良好市场份额的获取提供了强有力的基础和资源保障。

不断提升的差异化服务，建立用户口碑——通过以客户为中心，研发生态圈角进行服务满意度测评，收集内部及外部对产品和服务方面的建议意见，识别客户关键问题，推动产品和服务改进，确保客户各项问题得到及时有效反馈，客户满意度提升。

行业领先的品牌影响力——作为国内网络安全领域的领导者之一，在进行研发创新和市场开拓的同时，公司积极推进国家信息技术及信息安全技术相关标准规范的编制、推广和落地等工作，努力促进行业规范有序发展。

深信服2021年年报

奇安信科技集团股份有限公司【688561】

企业状态：存续
注册资本：68208.2124万人民币
企业总部：深圳市
行业：科技推广和应用服务业
法人：齐向东
统一社会信用代码：91110105397625067T
企业类型：其他股份有限公司(上市)
成立时间：2014-06-16
经营范围：互联网网络安全技术服务；技术开发、信息技术咨询、技术推广、技术转让；计算机系统服务；信息处理和存储支持服务；信息系统集成；销售通信设备、电子产品、计算机软硬件及辅助设备；软件开发；互联网数据服务；数据处理；会议服务；承办展览展示活动；货物进出口；技术进出口；代理进出口；设计、制作、代理、发布广告；出版物零售。（市场主体依法自主选择经营范围，开展经营活动；出版物零售等以及依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动；不得从事国家和本市产业政策禁止和限制类项目的经营活动。）
股票类型：科创板
品牌名称：奇安信科技集团股份有限公司
：

奇安信科技集团股份有限公司财务数据分析

财务指标	2017	2018	2019	2020	2021	2022(Q1)	2022(Q2)
销售现金流/营业收入	1.25	1.02	0.91	0.88			
营业收入同比增长(%)	37.5659	36.9255	29.5498	19.3336	26.495	27.351	30.818
营业收入同比增长(%)	121.2221	73.6116	31.9278	39.602	44.521	35.207	
归属净利润同比增长(%)	-38.4058	43.2246	32.4438				
流动比率	1.3493	1.666	2.0266	3.8819	2.79	2.6	2.19
每股经营现金流(元)	-23.21	-6.4	-1.93	-1.0132	-1.909	-1.421	-2.183
毛利率(%)	74.9074	55.6849	56.724	59.5723			
流动负债/总负债(元)	97.0365	95.6549	93.096	92.9121	83.256	84.544	86.304
经营现金流/营业收入	-23.21	-6.4	-1.93	-1.0132	-1.909	-1.421	-2.183
基本每股收益(元)	-1.67	-1.78	-0.9	-0.54	-0.82	-0.7	-1.34
净利率(%)	-85.5178	-52.4289	-17.5316	-8.1885	-9.5363	-73.1821	-46.3014
总资产周转率(次)	0.1557	0.3013	0.4526	0.4251	0.448	0.05	0.149
存货周转天数(天)	784.8267	236.9512	179.3097	144.945	110	289	173
营业收入收入(元)	8.214亿	18.174亿	31.544亿	41.614亿	58.094亿	6.594亿	19.684亿
稀释每股收益(元)	-1.67	-1.78	-0.9	-0.54	-0.82	-0.7	-1.34
每股公积金(元)	181.2034	38.9252	11.441	17.3553	17.8804	17.9284	18.0004

奇安信科技集团股份有限公司竞争优势

开创性的网络安全建设理念——公司开创性地提出了“内生安全”的核心理念，重塑网络安全体系，从过去的“局部整改”、“事后补救”的外挂式建设模式走向“深度融合”的体系化建设模式，改善网络安全体系化建设、碎片化严重、协同能力差的旧有局面，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

强大的安全防护技术——公司已建成全链条以防为核心的技术能力体系，从漏洞挖掘与利用，到攻击检测与响应，恶意样本分析与查杀、威胁情报与反制、攻击追踪与溯源，再到威胁情报、全网态势感知、APT组织监控及电子取证等环节，均取得出色的成绩。

强大的研发能力与平台能力——公司在多个网络安全技术领域，研发并推出了一系列具有技术创新优势的产品、方案和服务，在云安全、大数据安全、物联网安全、移动互联安全、人工智能应用安全等新兴领域全面布局，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

全面丰富的网络安全产品体系——公司丰富的产品体系能够内生于客户的各个关键信息化领域，与其信息化环境进行深度融合与覆盖，形成有效的、系统性的防护。

奇安信科技集团股份有限公司2021年年度报告

开创性的网络安全建设理念——公司开创性地提出了“内生安全”的核心理念，重塑网络安全体系，从过去的“局部整改”、“事后补救”的外挂式建设模式走向“深度融合”的体系化建设模式，改善网络安全体系化建设、碎片化严重、协同能力差的旧有局面，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

强大的安全防护技术——公司已建成全链条以防为核心的技术能力体系，从漏洞挖掘与利用，到攻击检测与响应，恶意样本分析与查杀、威胁情报与反制、攻击追踪与溯源，再到威胁情报、全网态势感知、APT组织监控及电子取证等环节，均取得出色的成绩。

强大的研发能力与平台能力——公司在多个网络安全技术领域，研发并推出了一系列具有技术创新优势的产品、方案和服务，在云安全、大数据安全、物联网安全、移动互联安全、人工智能应用安全等新兴领域全面布局，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

全面丰富的网络安全产品体系——公司丰富的产品体系能够内生于客户的各个关键信息化领域，与其信息化环境进行深度融合与覆盖，形成有效的、系统性的防护。

奇安信科技集团股份有限公司2021年年度报告

开创性的网络安全建设理念——公司开创性地提出了“内生安全”的核心理念，重塑网络安全体系，从过去的“局部整改”、“事后补救”的外挂式建设模式走向“深度融合”的体系化建设模式，改善网络安全体系化建设、碎片化严重、协同能力差的旧有局面，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

强大的安全防护技术——公司已建成全链条以防为核心的技术能力体系，从漏洞挖掘与利用，到攻击检测与响应，恶意样本分析与查杀、威胁情报与反制、攻击追踪与溯源，再到威胁情报、全网态势感知、APT组织监控及电子取证等环节，均取得出色的成绩。

强大的研发能力与平台能力——公司在多个网络安全技术领域，研发并推出了一系列具有技术创新优势的产品、方案和服务，在云安全、大数据安全、物联网安全、移动互联安全、人工智能应用安全等新兴领域全面布局，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

全面丰富的网络安全产品体系——公司丰富的产品体系能够内生于客户的各个关键信息化领域，与其信息化环境进行深度融合与覆盖，形成有效的、系统性的防护。

奇安信科技集团股份有限公司2021年年度报告

开创性的网络安全建设理念——公司开创性地提出了“内生安全”的核心理念，重塑网络安全体系，从过去的“局部整改”、“事后补救”的外挂式建设模式走向“深度融合”的体系化建设模式，改善网络安全体系化建设、碎片化严重、协同能力差的旧有局面，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

强大的安全防护技术——公司已建成全链条以防为核心的技术能力体系，从漏洞挖掘与利用，到攻击检测与响应，恶意样本分析与查杀、威胁情报与反制、攻击追踪与溯源，再到威胁情报、全网态势感知、APT组织监控及电子取证等环节，均取得出色的成绩。

强大的研发能力与平台能力——公司在多个网络安全技术领域，研发并推出了一系列具有技术创新优势的产品、方案和服务，在云安全、大数据安全、物联网安全、移动互联安全、人工智能应用安全等新兴领域全面布局，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

全面丰富的网络安全产品体系——公司丰富的产品体系能够内生于客户的各个关键信息化领域，与其信息化环境进行深度融合与覆盖，形成有效的、系统性的防护。

奇安信科技集团股份有限公司2021年年度报告

开创性的网络安全建设理念——公司开创性地提出了“内生安全”的核心理念，重塑网络安全体系，从过去的“局部整改”、“事后补救”的外挂式建设模式走向“深度融合”的体系化建设模式，改善网络安全体系化建设、碎片化严重、协同能力差的旧有局面，并获得业界认可，公司产品逐步打造八大研发平台，助力网络安全行业走出开发成本、周期长、扩展性差、盈利能力弱的怪圈，避免了不同产品适用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品品质，更好满足政府、企业客户持续变化的个性化需求。

强大的安全防护技术——公司已建成全链条以防为核心的技术能力体系，从漏洞挖掘与利用，到攻击检测与响应，恶意样本分析与查杀、威胁情报与反制、攻击追踪与溯源，再到威胁情报、全网态势感知、APT组织监控及电子取证等环节，均取得出色的成绩。

强大的研发能力与平台能力——公司在多个网络安全技术领域，研发并推出了一系列