平安证券

计算机

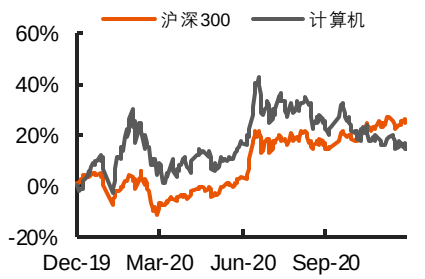
2021 年 2 月 9 日

行业深度报告

网络安全：关注新变化，聚焦新赛道

强于大市（维持）

行情走势图



证券分析师

付强 投资咨询资格编号
S1060520070001
fuqiang021@pingan.com.cn

闫磊 投资咨询资格编号
S1060517070006
010-56800140
yanlei511@pingan.com.cn

- **2021 年网络安全面临的新变化、新挑战。**2020 年岁末，全球影响最大的一系列攻击事件浮出水面，美国财政部、商务部等多个政府机构用户遭到入侵和监视，多家商业公司如微软、英特尔、思科、VMware 等也称遭受到了入侵。而攻击的起源则是 IT 供应商 SolarWinds 更新服务器被侵入并植入恶意代码，进而影响到其大量客户。这是一次具有一定战略性质的 APT（高级可持续性威胁）攻击，给全球的网络安全防御体系敲响了警钟。这次事件说明，安全防护的边界正在超越 IT 系统本身，安全产品的防御正面在持续扩大，安全行业也需要做针对性的改变。同时，新技术的滥用、新场景安全防护能力的薄弱，也给整个安全市场带来了新的威胁。此外，各国开始收紧网络安全监管，国内积极参与塑造网络空间治理新秩序。

- **网络安全市场转型加速，新安全、新服务成为主引擎。**网络安全行业的发展一直是威胁、技术和监管等多方博弈的结果，最终达到一个均衡。新的威胁、技术以及新的监管要求，都会带来市场需求的增长。客户需求从以前的合规为主，逐步开始重视攻防实效，关注安全产品和服务能否实现对云计算、大数据、工业互联网等新场景进行有效防护，保证系统和数据资产的安全。因此，我们也看到，在国际咨询机构 Gartner 的报告中，云安全、数据安全等新安全一直是全球安全行业中增长最快的领域，国内企业如深信服、安恒信息等，就在持续深耕这些板块，相关产品和平台具有较强的市场竞争力，受益最为明显。安全服务在国内市场上也开始受到重视，客户对安全服务的接受度提升。传统安全企业积极寻求转型，在探索工业互联网安全等新安全市场的同时，积极布局服务市场，进展也较为明显。

- **云安全等新赛道在国际市场上已得到成功验证，国内转型适逢其时。**相较而言，国内网络安全产业还在起步阶段，安全投入和技术同国际先进水平还有较大差距。从新技术应用和发展阶段角度看，国内还处在追赶状态，国际安全企业的成功经验也可供国内安全企业参考。近年来，在国际市场上，传统安全企业如 Palo Alto Networks、Fortinet 等均在向云安全、数据安全市场转型，并取得了积极效果。同时，在美国市场涌现出来的一些专业企业如 Zscaler、Crowdstrike 等，在云安全、终端安全等方面均形成了独特的竞争力，并持续受到市场的热捧。国际市场上，传统企业转型成功以及新兴企业的崛起，证明了走“新安全”这条路是可行的。国内无论是新安全企业继续拓展还是传统企业向该领域转型，成功的几率均较高。

- **投资建议：**随着数字经济发展的提速，云安全、数据安全将面临着巨大的发展机遇，国内一些新兴安全企业有望实现跨越式发展，传统安全龙头也有望在这一轮洗牌中实现蜕变。云安全板块，推荐深信服，公司是国内私有云解决方案和网络安全的“双料”龙头企业，云和安全的协同性较好，云安全产品具有较强的竞争力。数据安全和工控安全板块，推荐安恒信息，

关注奇安信。安恒信息自数据库安全起家，态势感知、AiLPHA 大数据智能安全平台都表现出良好的增长势头；奇安信在基于大数据的检测控制、分析与监测等安全产品上具有较强的竞争力，而且在工控态势感知平台的建设上也取得了积极进展。

- **风险提示：**1）竞争加剧的风险。随着新安全市场的发展，不同背景的安全厂商同台竞争的可能性增大，比如互联网、传统 ICT 企业等，技术、品牌、人才和资金等方面的竞争加剧，行业总体和企业毛利率都存在下降的风险。2)技术风险加剧。新领域的安全防护能力建设需要的是持续的研发投入，我国在新安全领域的研发同国际巨头还存在较大的差距，研发方向选择失误或者研发进度不及预期，都可能对企业短期业绩和长期发展带来不利影响。3）客户安全支出不及预期。行业客户多采用预算制进行产品和服务采购，宏观经济环境如出现不景气可能影响部分行业客户的 IT 投资预算。2021 年以来，其他国家新冠疫情仍在蔓延，中美经贸关系也存在较大不确定性，国内经济增长仍面临较大压力，政企客户信息安全投入可能被迫下调或者推迟。

股票名称	股票代码	股票价格	EPS				P/E				评级
		2021-2-8	2019A	2020E	2021E	2022E	2019A	2020E	2021E	2022E	
安恒信息	688023	247.00	1.24	1.39	1.87	2.47	199.19	177.70	132.09	100.00	推荐
深信服	300454	308.90	1.83	1.94	2.53	3.31	168.80	159.23	122.09	93.32	推荐
奇安信-U	688561	105.80	-0.73	-0.45	0.06	0.66	-144.93	-235.11	1763.33	160.30	未评级

注：未评级报告采用 Wind 一致预期

正文目录

图表目录

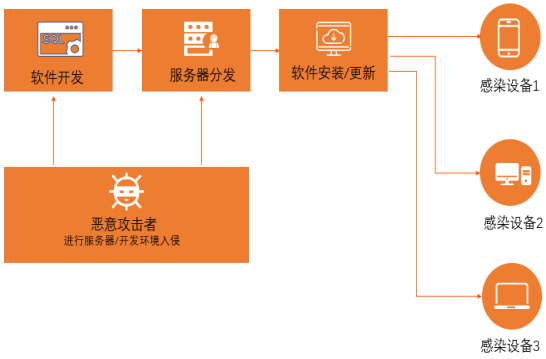
一、 2021 年网络安全面临的新变化、新挑战

2020 年岁末，全球最严重的一连串攻击事件浮出水面。该系列攻击事件发酵于 2020 年 12 月中旬，知名 IT 公司 SolarWinds 旗下的 Orion 网络监控软件更新服务器，被发现遭黑客入侵并植入恶意代码，美国财政部、商务部等多个政府机构用户遭到入侵和监视，此外多家商业公司如微软、英特尔、思科、VMware 等也都遭受到了入侵。这次具有一定战略性质的 APT（高级可持续性威胁，下同）攻击，给全球的网络安全防御体系敲响了警钟。这次事件说明，安全防护的边界正在超越 IT 系统本身，安全产品的防御正面在持续扩大，安全行业也需要做针对性的改变。

1.1 安全威胁呈现出新特点，技术含量高、隐蔽性强且破坏性极大

SolarWinds 遭受的攻击影响面大且破坏性高，但依然只是 2020 年众多网络攻击的冰山一角。SolarWinds 是全球重要的网络及系统管理工具型软件，黑客将该软件污染之后，就可以渗透进其客户网络，实现窃取用户资料、破坏用户系统等目的。这种利用用户 IT 供应链上某一个环节进行的网络攻击，我们称之为供应链攻击。由于大型、具有战略价值的 IT 业主，都有着庞杂的 IT 供应链体系，而供应链某些脆弱环节，非常容易被当成黑客组织攻击业主 IT 系统的跳板。SolarWinds 此次遭受的攻击，黑客组织利用的就是它的网络及系统管理工具这类高权限模块，可以完全绕过用户 IT 系统内部的等级防护，实现长期匿名潜伏并访问被攻击者的网络，进而伺机获取客户信息。

图表1 供应链攻击发生过程



资料来源:深信服千里目实验室、平安证券研究所

图表2 供应链攻击发生的各个环节

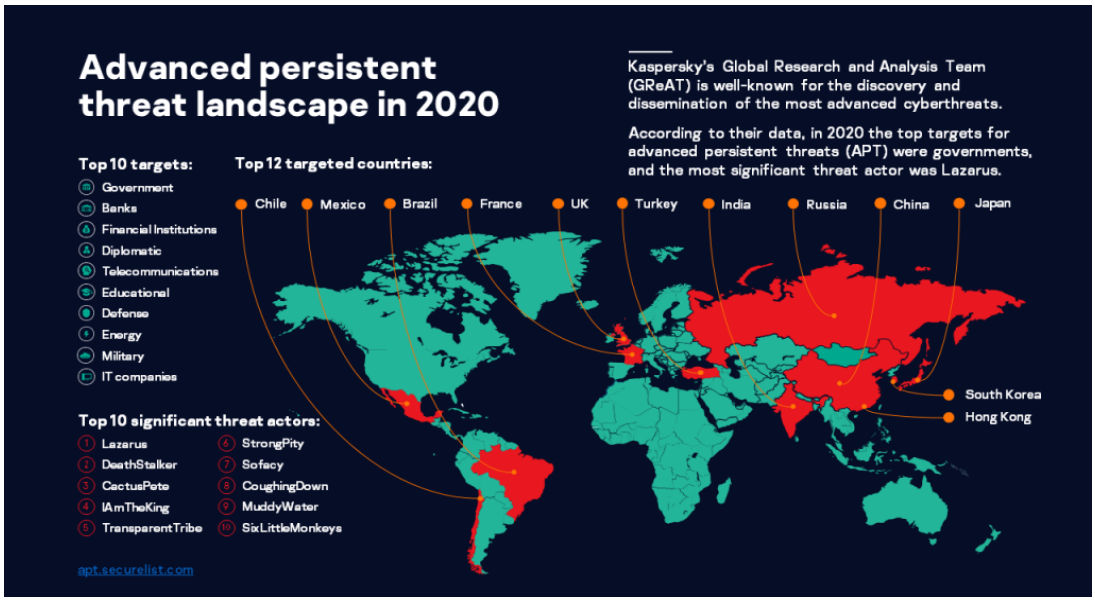
资料来源:百度文库、平安证券研究所

类似于供应链攻击这种组织性强、技术含量高、潜伏时间长、攻击手段隐蔽的网络攻击手段，我们称之为高级可持续性威胁攻击（APT）。这种有组织的攻击能够绕过现有防护体系，攻击和威胁在用户环境中长期潜伏甚至一年以上。黑客“攻陷”或者控制的主机一般只是作为跳板，通过该“跳板”持续尝试多种攻击手段，“嗅探”客户的高价值数字资产，最终实现窃取或者破坏的目的。这种攻击同传统黑客单打独斗炫技不同，目标明确并且组织性极强，而且部分还有政府背景，目前发现的比较活跃的 APT 组织包括摩诃草、蓝宝菇、毒云藤、蔓灵花、海莲花、Darkhotel 等。

2020 年以来，全球网络环境中各类 APT 组织均十分活跃，攻防趋于白热化，攻击的对象已经不仅限于传统的 PC 和服务器，已经拓展到暴露在网上的互联网应用、互联网新业务（区块链等）、移动应用、物联网等。攻击的目标除了企业之外，政府机构和关键基础设施也都处在风险之中，包括电力、电信等民生基础设施等。2020 年以来，新冠疫情暴发、中印边界争端以及重大会议等特殊时期，针对我国的 APT 攻击明显趋于活跃，政府机构、金融、军工以及医疗机构等成为了主要攻击目标。

正是因为 APT组织技术快速演变和攻击能力在持续加强，我国面临的安全威胁更大。随着新基建投资的加快，国内各类 IT 系统建设正在提速，但我们的基础软硬件依然严重依赖全球供应链。而在 SolarWinds 遭受的攻击事件中，我们看到，IT 供应链中的顶级软、硬件企业都受到影响，我国很难独善其身。由于我国还不能真正实现关键领域的自主可控，一旦遭受攻击，由于不掌握底层架构，很难在第一时间对漏洞进行封堵，不光是企业商业利益可能受损，国家安全都有可能受到威胁。因此，相比其他国家，我们在面对此类攻击的过程中，需要做的更多，不光是需要做好系统的安全防护，还需要打造自主可控的产业链条，由内而外的通过整个“体系”解决问题。

图表3　2020 年全球 APT 攻击的目标国分布情况



资料来源:卡巴斯基实验室、平安证券研究所

1.2 新技术滥用、新场景防护能力弱，网络攻击手段更为复杂、影响更广

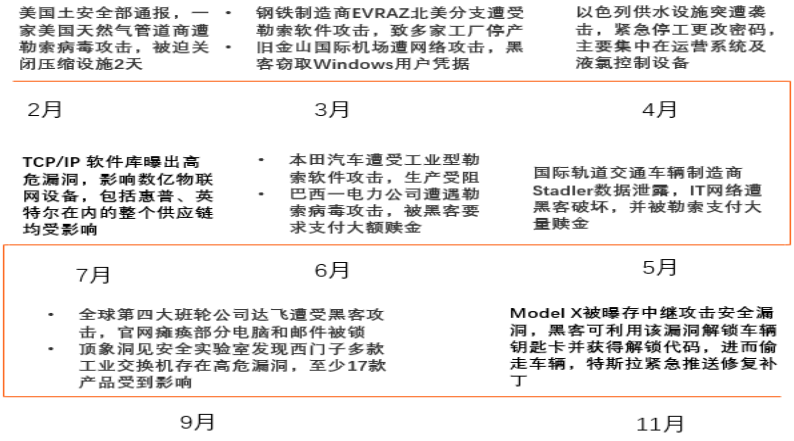
人工智能、量子计算等新技术在推动信息技术产业变革的同时，也存在被黑客利用的风险。这些技术正在被应用到网络攻击的自动化、智能化等领域。除了当前业界高度关注的 APT、勒索软件、内部威胁和 DDoS 攻击之外，这些新技术还广泛应用于猜测密码、破解验证码等领域。其中，人工智能更是广泛应用于训练数据污染、机器学习攻击等新型网络犯罪行为中，而且很多恶意创新尚未为人所知。新技术一旦成为网络攻击的工具，这将引发网络攻防形势的变化。同时，安全防护理念、思路和技术实现路径都需要进行动态的调整、适配。以前重系统、轻业务的模式需要彻底改变。

据 Beyondtrust 在 2020 年发布的最新预测报告显示，污染机器学习的训练数据已经成为黑客组织新的攻击手段。黑客组织通过盗取系统的原始训练池的数据进行再训练，并在训练池中加入有害数据，最终形成存在人为漏洞的系统，通过系统更新分发至客户，进而埋下安全隐患。Beyondtrust 同时指出，黑客也正在利用机器学习加速针对网络和系统进行攻击，机器学习引擎开始尝试使用“攻击成功”的数据进行训练，借此识别客户网络防御体系的防护模式，快速找到系统和环境中的漏洞，而且这些数据可以继续应用于后续的训练。通过类似方式，攻击者可以更快、更隐蔽地进行攻击，而且确保每次攻击只涉及很少的漏洞，避免大面积尝试被安全工具所发现。

新技术也催生了新的安全应用场景，而这些新领域的安全防护本身相当脆弱，防护正面明显扩大。当前，新一代信息技术正在同经济社会发生更广范围、更深层次和更高水平的融合，但网络安全的

风险也在不断渗透、扩散和放大，尤其是在工业互联网、区块链、物联网、车联网等新场景，安全防护的压力更大。随着 5G 与工业互联网应用结合的提速，整个工控领域的信息化水平大幅提升，但相关的安全风险也在加剧。一般而言，工控设施数据敏感价值高，但由于系统漏洞较多，攻击低成本、高收益，成为近年来黑客组织重点“关照”的领域。全球看，2020 年，天然气、机场、水电等设施都遭受到了不同类别的攻击，同时一些主流的工控系统也爆出高危漏洞，给工控安全造成极大的隐患。新的场景带来了新的脆弱性，需要整个产业链共同努力，提前布局，有效防范不断变化的风险。

图表4 2020 年以来全球主要国家工控威胁典型事件



资料来源:威努特工控安全、平安证券研究所

1.3 各国收紧网络安全监管，国内在积极努力塑造网络空间治理新秩序

监管对安全防护要求的提升是各国网络安全投资的重要推手，传统网络安全支出很大一部分都是为了应对监管而产生。全球来看，网络安全环境趋于复杂，尤其是棱镜门以来，各国对网络安全的重视程度明显提升，部分国家甚至开始将信息安全或者网络安全泛化，将本属于科技领域的问题政治化，以打击战略竞争对手。更有甚者，一些西方国家开始将网络安全技术武器化，建立网空部队打造武器库。疫情以来，全球重大网络安全事件中，很多都有国家力量的影子。根据 CSIS 网络事件报告梳理统计，2020 年有国家支持背景的网络攻击高达 112 起，主要包括疫苗信息窃取、外交政策情报获取、军事报复、商业行为等。前文提到的 SolarWinds 所遭受到的攻击，因为针对的也是美国重要的政府或者商业机构，美方也在怀疑背后是否有政治力量在支持。

2020 年新冠疫情的爆发，使得各国在网络安全监管上的动作更为频密。我们看到，虽然疫情这只黑天鹅给传统经济带来了巨大冲击，但也带来了数字经济的繁荣，尤其是线上经济成为了新常态。数字经济的发展，也带来相关国家对数据安全的关注。2020 年，《G20 数字经济部长宣言》《区域全面经济伙伴关系协定》（RCEP）对疫情期间的新兴技术使用、数据安全均提出了倡议。美国开始重新利用多边机制实现自身诉求，包括加入七国集团“人工智能全球合作伙伴组织”，推动亚太经合组织修改有关个人数据规则的方案。欧盟 2020 年初连发《塑造欧洲的数字未来》《人工智能白皮书》《欧洲数据战略》三部文件，称将全面落实其“技术主权”和“数字自治”理念，并首次使用“网络外交工具箱”对多国实施制裁，高调宣示其战略自主。脱欧后的英国频繁在国际网络治理热点问题上发声，推动组建“D10”5G 国际俱乐部，加强与美国、日本等国的网络安全合作，将网络治理作为

参与国际事务的“破局之道”。但是，我们也看到，2020 年各家在监管方面动作都比较多，但是多呈现出自说自话的状态，诉求不一、愿景不同，整体网络空间治理成效十分有限。

我国在主动塑造网络空间治理新秩序的同时，也在积极准备法律和政策工具，做好自己的事情，以应对来自各个方向的挑战和风险。习总书记“4.19”讲话指出，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。2020 年，监管部门继续在扎紧制度的篱笆，加快落实《网络安全法》要求推动等级保护和关键基础设施保护，出台《网络安全审查办法》完善供应链审核以树立网空安全屏障；2021 年我国还有望在个人数据保护立法方面取得进展，同时更加关注底层软硬件的技术和供应链安全。但是，我们也看到，国内网络安全体系建设还处在起步阶段，离全面“安全可靠”还有很长的路要走。从 2021 年的重点来看，政企全面态势感知能力要增强，同时网安工作的重心还要从“被动防御”转向到“主动防御”上来，攻防演练等工作将成为常态化。

二、 网络安全市场转型加速，新安全、新服务成为主引擎

2.1 威胁、技术和监管等因素倒逼市场改变，供需双方将更加注重攻防实效

网络安全行业的发展一直是威胁、技术和监管等方面相互博弈的结果，最终达到一个均衡。新的威胁、技术以及新的监管要求，都会带来市场需求的增长。而对安全企业来说，需要密切关注这些力量的变化，推出适合的产品和服务，这样才能在市场上处于不败之地。

安全需求端确确实实在发生变化，更加注重攻防实效。21 世纪初，我国信息化和互联网建设提速，政企投入的重点主要集中 IT 系统的建设，针对用户的攻击多为黑客炫技或者个人行为，对整个系统的影响并不明显，政企的安全意识还在教育和培育之中，安全投入主要是为了应付监管和突发安全事件，在多数行业还是“可选”状态。但随着时间的推移，政企数字化水平持续提升，IT 系统上沉淀的数字资产越来越多，攻击回报日趋丰厚，黑产开始兴起，攻击开始呈现出组织化、手段也在趋于高端化，而在这个时期政企安全投入开始提升，而且关注的重点不光是“筑高墙”，尤其是勒索病毒猖獗之后，内网终端、态势感知等方面的投入也在增加。除此之外，随着信息化应用的深化，针对云计算、大数据平台、工控和物联网等防护方面的需求也在增加，尤其是在工控和物联领域，由于协议的复杂性，定制化的安全防护需求更多。总体上看，由于安全防护的重点在变化，由系统变为了防护资产，因此客户更关注的是防护的实效，对能够解决自身“痛点”的安全解决方案或者服务更为青睐。

供给侧也在开始调整，针对合规、场景和技术推出新的产品和服务。合规方面，几乎所有的网络安全公司都针对等级保护推出了相应解决方案，实力较强的龙头企业也在积极参与到关键基础设施保护当中。针对新场景，新兴的安全企业的优势正在凸显出来，传统安全企业正在向这个方向转型。同时，安全厂商也在注重应用新技术为客户赋能，比如区块链和人工智能技术等。其中，区块链技术推动数据存储方式转型和信任机制重塑，目前已应用于无密钥的签名方案、强认证的安全数据存储等安全场景中。人工智能技术能够更快、更精准、更全面的进行采集和分析，提高攻击威胁等的监测、识别、响应效率，目前已在入侵检测、恶意软件分类、用户行为分析、攻击智能感知等方面取得积极进展。针对疫情以来的线上办公场景，安全厂商为了应对这种网络安全边界的模糊化，成功将零信任由概念转向落地，部分厂商的解决方案还取得了不错的效果。除了上述的变化之外，各大厂商也在加大安全服务业务的布局。

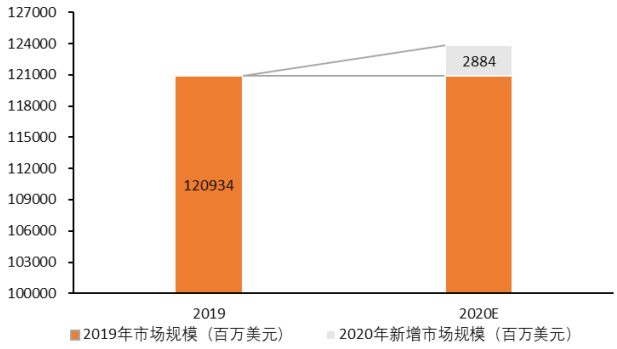
图表5 网络安全市场发生的新变化

资料来源:平安证券研究所

2.2 云、数等新安全市场强劲爆发，深信服、安恒信息等龙头厂商充分受益

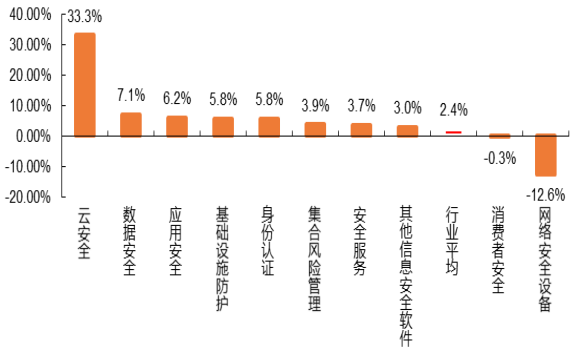
云计算、数据安全是 2020 年安全市场比较亮眼的点。一方面，是由于数字化转型和线上经济爆发的推动；另一方面，是安全发展的新趋势使然，行业只有契合新场景的需要，才能在数字化的大趋势下，伴随着用户的成长而获得发展。按照 Gartner 的测算，云安全、数据安全成为 2020 年增长的主要动力，其中云计算安全增长最快，增速预计超过 30%。从国内安全企业发展来看，一些在云计算、数据安全布局较早的企业，市场竞争优势已经凸显出来，尤其是这种非常时期，凭借完整的平台体系和技术能力，相关业务板块均获得了快速增长。相反，据 Gartner 的预测，包括防火墙、IPS/IDS 等传统网络安全产品在内的网络安全设备，2020 年可能出现较为明显的下滑。

图表6 2019-2020 年全球网络安全市场规模及预测



资料来源:Gartner 预测（2020.6）、平安证券研究所

图表7 2020 年全球网安主要板块市场规模预计增速



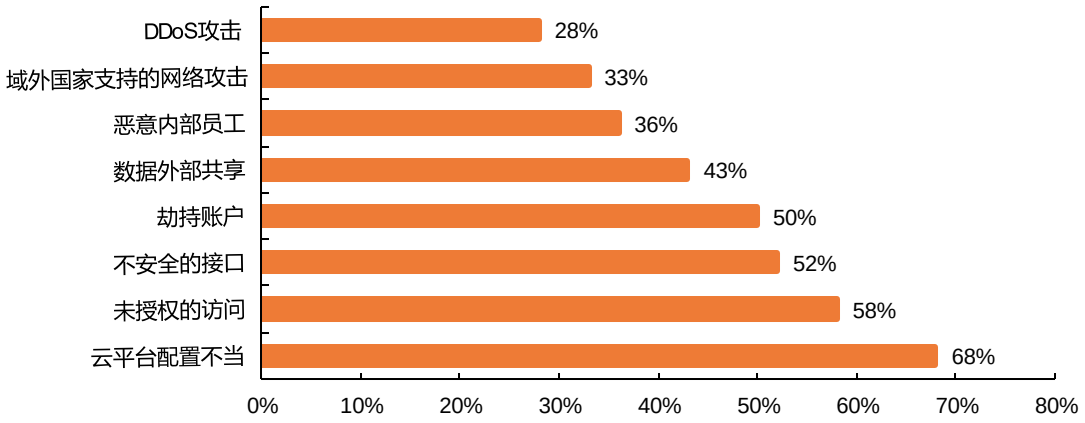
资料来源:Gartner 预测（2020.6）、平安证券研究所

云安全将成为网络安全增长最快的领域

云安全是伴随着云计算的快速发展而成长起来，并保持着积极发展势头。随着政企业务和个人应用上云的加速，云计算平台的脆弱性开始显现，基于云计算或者针对云计算平台的攻击也开始增多，市场上对云安全的关注度持续提升，并快速转化成 IT 投入，客观上拉动了云安全市场的快速发展。从供给端来看，随着硬件虚拟化技术的成熟，将传统的安全能力云化，为云上用户提供安全防护和管理；从用户端看，通过云安全管理工具和平台，客户可以实现安全能力的自助化部署、弹性扩容、按需分配、统一运维，这样可以降低用户的前期设施投入和后续的运营成本。

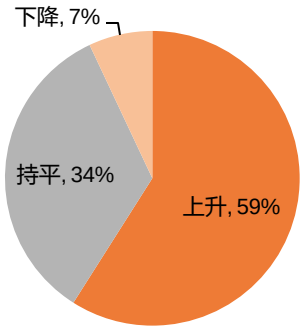
按照 Gartner 报告统计，2019 年网络安全交付模式中，通过云进行的安全交付占到 12%；在一些关键安全市场上，包括安全邮件、网关等，采用云上交付的占到 50%。此外，据 CyberSecurity Insiders 发布的《2020 年全球云安全报告》显示，调研的 94%的安全专业人士开始不同程度的关注公有云安全，而且超过 82%认为单纯将传统安全软件移植到云上并不能很好的解决问题，云原生的安全方案更受青睐。同时，在 CyberSecurity Insiders 的报告中也指出，调查企业安全预算中有 27%在投向云安全，59%的企业未来 12 个月内会增加云安全预算（该调研报告发布时间为 2020 年 8 月）。

图表8 云计算面临的安全威胁



资料来源: CyberSecurity Insiders、平安证券研究所

图表9 未来 12 个月云安全预算变化情况

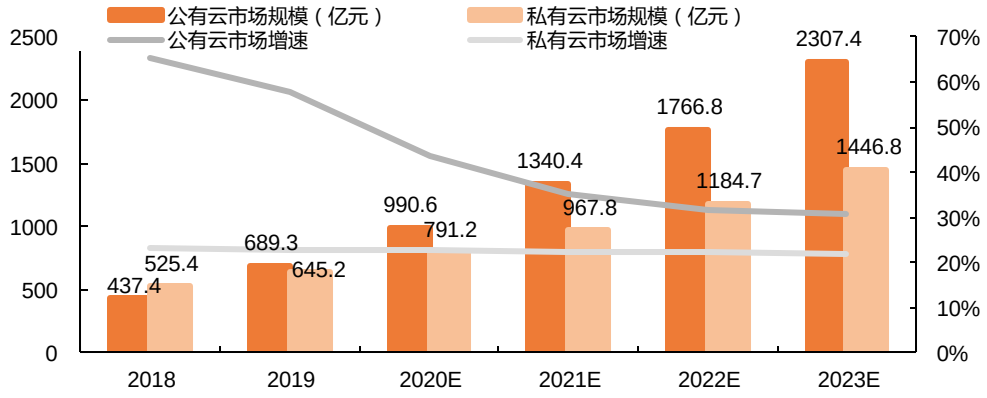


资料来源: CyberSecurity Insiders（2020.8）、平安证券研究所

国内云安全市场目前正处在高速增长阶段，市场格局也正在趋于多元，第三方网络安全厂商的影响力有所扩大。云安全的概念起源于美国安全公司趋势科技（2008 年），而国内云安全产业萌发则比美国慢 2-3 年，2011 年左右一些创业公司开始进入，2014 年左右阿里云、华为、百度、腾讯等云厂商推出了云安全服务，作为安全责任第一责任人，云服务商的安全能力也一直是行业内最强的。此后传统安全企业也开始上线云安全服务，此后进入快速发展期。

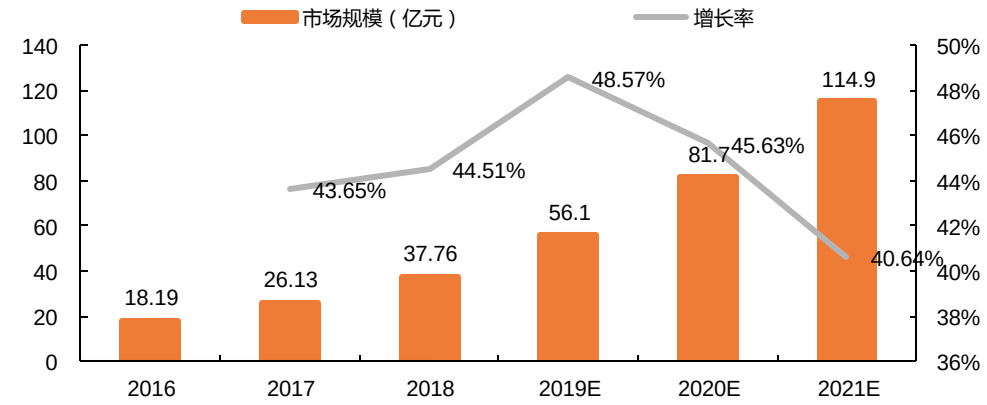
目前，行业已经形成了以云服务商、安全厂商、初创企业为主要参与者的市场格局，多方在行业快速发展的过程中受益。据信通院最新报告预测，2020 年国内公有云和私有云市场规模将分别达到 1340.4 亿和 967.8 亿元，同比分别增长 43.7%和 22.6%，增长非常迅速。据赛迪预计，2020 年国内云安全市场将有望达到 80 亿元，增速将维持在 40%以上。

图表10　2020-2023 年国内公有云、私有云市场规模及预测



资料来源:信通院、平安证券研究所

图表11　2016-2021 年我国云安全市场规模及预测



资料来源:赛迪、平安证券研究所

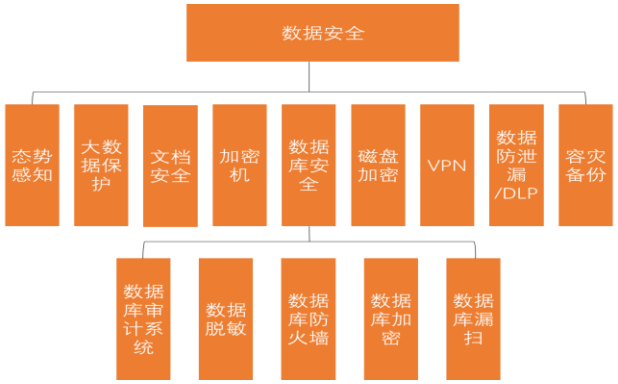
数据安全重视程度明显提升

除了云安全之外，数据安全也是近年来网络安全行业关注的热点。随着云计算和大数据技术的快速发展和广泛应用，尤其是客户业务体量达到一定规模以后，数据的产生、流通和应用更加普遍化和密集化，数据作为企业的资产属性也越来越强。然而，伴随着数据价值的提升，相关的黑产也快速蔓延，针对企业数据资产的攻击也是层出不穷，相关的数据泄露事件时有发生。面对海量数据处理

的场景，数据治理难度十分复杂，传统的网络安全产品难以满足需求，安全防护的理念也正在发生变化。从 2020 年安全牛调查的数据显示，全部信息安全的 72 个细分领域中，排在前三位均和数据安全相关，分别是大数据安全、数据防泄漏 DLP、隐私增强。除了客户现实需求之外，来自监管侧压力也在增加，欧洲、美国已经明显加强对数据管控，我国对数据安全的立法也正在路上，《数据安全管理办法》已经在 2019 年公开征求意见，《数据安全法（草案）》也将成为 2021 年人大常委会审议的重点，相关法律法规都有望在短期内出台。

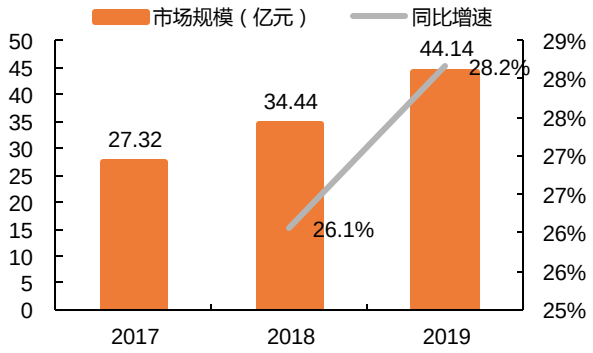
数据安全在国内成长比较迅速，但是尚未形成完整的解决方案，各厂商的视角存在较大差异，很多厂商都是围绕着数字周期的某一个阶段进行防护，优势厂商的产品相对丰富一些。从分类来看，主流的数字安全分为四类：1）数据库安全，这是面向合规的刚需市场，政策规范也相对清晰，市场规模较大，但是竞争也趋于激烈；2）数据防泄漏方向，包括主机数据防泄漏和网络数据防泄漏产品，这类产品在企业数字化转型和企业上云的大潮中应用较多，市场增长较快；3）数据加密方向，包括电子文档加密、磁盘/存储介质加密、应用加密等产品，这类产品在商业市场、信创市场有着广泛的应用；4）数据合规与治理方向，包括敏感数据发现、数据分级、数据清理等方案。除了这四类主流分类之外，很多厂商将态势感知这类基于大数据平台等技术的安全系统也放在数据安全门类之下。

图表12　数据安全行业细分技术



资料来源:安全牛、平安证券研究所

图表13　2017-2019 年数据安全市场规模及增速



资料来源:安全牛、平安证券研究所

注：数据安全市场规模不包括综合安全公司的数字安全业务部分，且不包含态势感知。

数据库存放着政企的业务数据，因此也是公司数字资产的核心，如果数据遭受到篡改、破坏或者窃取，对相关组织可能造成较大伤害，甚至影响到国家安全，因此也是数据安全关注的重点。2020 年 2 月 28 日，国内微信头部提供商微盟，其生产数据库就遭到内部员工的恶意删库，虽然公司后续将数据恢复，但是公司的经营和声誉都受到了严重影响，数据库的安全性开始备受关注。近年来，该行业出现了两个方面的变化：一是国产数据库开始受到重视，除了武汉达梦、人大金仓、南大通用和神州通用等关系型数据库之外，阿里、腾讯、华为和中兴等都在入局，自主产品生态开始活跃，本质安全性在上升；另一方面，数据库安全厂商的能力也在增强，数据安全防护和审计的产品也开始成熟，安全解决方案的供给能力逐步在提升。

深信服、安恒信息等在云安全和数据安全市场上受益预计最为明显

➢ **云安全**

针对云计算场景，第三方厂商一般提供的是一个大的安全资源池或者云安全管理平台，实现安全资源的统一管理、弹性扩容、按需分配。从技术上来看，安全资源池通过虚拟化，将物理资源虚拟化成为资源池，提供云监测、云防御、云审计等能力；云安全管理平台则是强调对云安全资源的调配，包括自助开通、统一运维、自动编排、策略管理、资产管理、状态监控、数据分析等。另外，一些

第三方安全公司正在将自身竞争力较强的安全工具独立在云计算场景中应用，比如云抗 DDoS、云数据库审计以及云 WAF 等。

图表14 典型云安全管理平台主要功能（安恒天池云）

资料来源:安恒信息、平安证券研究所

目前，云安全上市的综合厂商包括深信服、奇安信、启明星辰、绿盟科技等。相关公司通过持续研发投入，已经形成了较为健全的产品体系，尤其是深信服，本身就是国内重要的私有云供应商，其云安全方案在市场上得到了广泛的应用；安恒信息等新兴安全公司，在云安全领域的投入也非常大，战略关注度也高，在云计算安全市场竞争中不落下风。

主要安全厂商的云计算安全业务均呈现出快速增长势头，并成为业务收入增长的重要动力。以安恒信息为例，公司基于其在云堡垒机、云数据审计等方面的能力，在 2016 年开始主要建立起安恒天池云安全管理平台，相关业务增长持续较快。2019 年，公司云安全平台业务实现收入 1.50 亿元，同比增长 176.25%。2020 年由于线上经济的爆发，国内云上安全业务需求延续高增长。安恒信息通过组织架构的调整，建立了安恒云事业部，战略重视程度和资源倾斜力度都在提升，我们预计公司云计算平台业务也将延续高增长势头。同样，综合安全龙头——奇安信，云安全业务收入也实现了快速增长。公司云安全业务主要得益于安全攻防倒逼出来的需求增长。按照公司业绩交流会公开纪要显示，2020 年前三季度，公司虚拟化安全、云安全管理平台、服务器防护等云安全需求大幅增长，收入增长 70%，远高于公司前三季度整体收入增速（30.41%）。

- **数据安全**

数据安全市场上，A 股上市公司主要就是安恒信息。安恒信息是从最为核心的数据库安全起家，已经形成了从基础产品到大数据安全平台的全栈布局。

数据库的风险来自外部攻击和内部越权访问两个方面，其中内部的越权访问占到攻击的 90%。内部威胁的源头主要来自于安全域划分的不规范、外包人员管理的混乱以及数据库访问工具的滥用等。数据库审计工具主要就是针对内外部的威胁所设计，通过大数据挖掘、审计取证、风险评估，最终进行安全告警并提出安全建议。安恒信息的数据库安全基础产品为明御数据库审计与风险控制系统。数据库对于公司管理者甚至 IT 人员来说，过于复杂，工作流程很难可知、可控，而安恒信息的数据库升级及风险控制系统就可以让数据工作全流程变为可视化。明御系统可以通过报文级别的数据库协议解析，完全还原出操作的细节，并给出详尽的结果。

除了数据库审计，公司也正在利用大数据技术，搭建安全平台，广泛应用于当前的攻防场景。公司类似的大数据安全平台有两个：1）网络安全态势感知通报预警平台。主要客户是网络安全监管和大型集团企业。平台利用多种威胁监测技术、大数据关联分析及机器学习技术，配合威胁情报数据服务，对其重要关键信息基础设施进行全面的画像、风险检测、攻击溯源。2）AiLPHA 大数据智能安全平台。主要客户为各类企业。该平台利用“AI 驱动安全”的核心理念，集成超大规模存查、大数据实时智能分析、用户行为分析、多维态势安全视图、企业安全联动闭环等安全模块，解决传统安全设备无法应对越来越复杂和隐蔽的安全威胁。

图表15 安恒信息网络安全态势感知通报预警平台

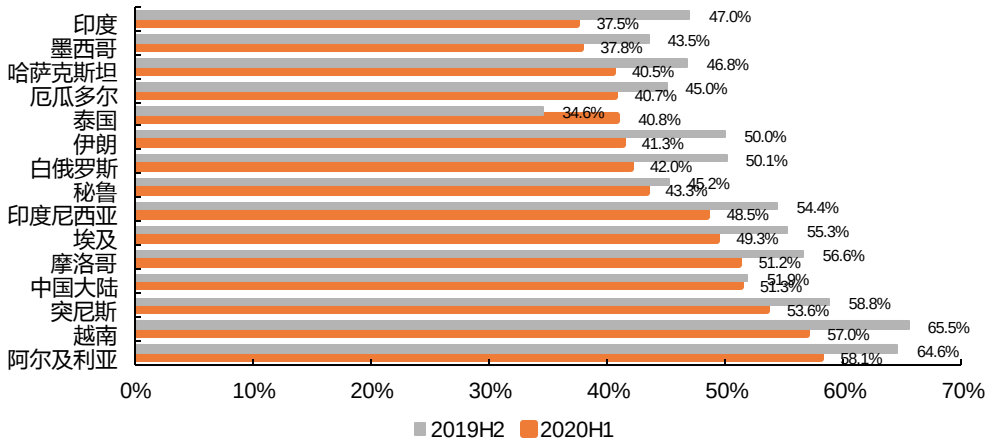
资料来源:公司官网、平安证券研究所

2.3 工控、安全服务等新领域需求旺盛，传统安全企业正在向此等领域转型

新基建加速工业互联网建设步伐，工控安全防护需求迫切

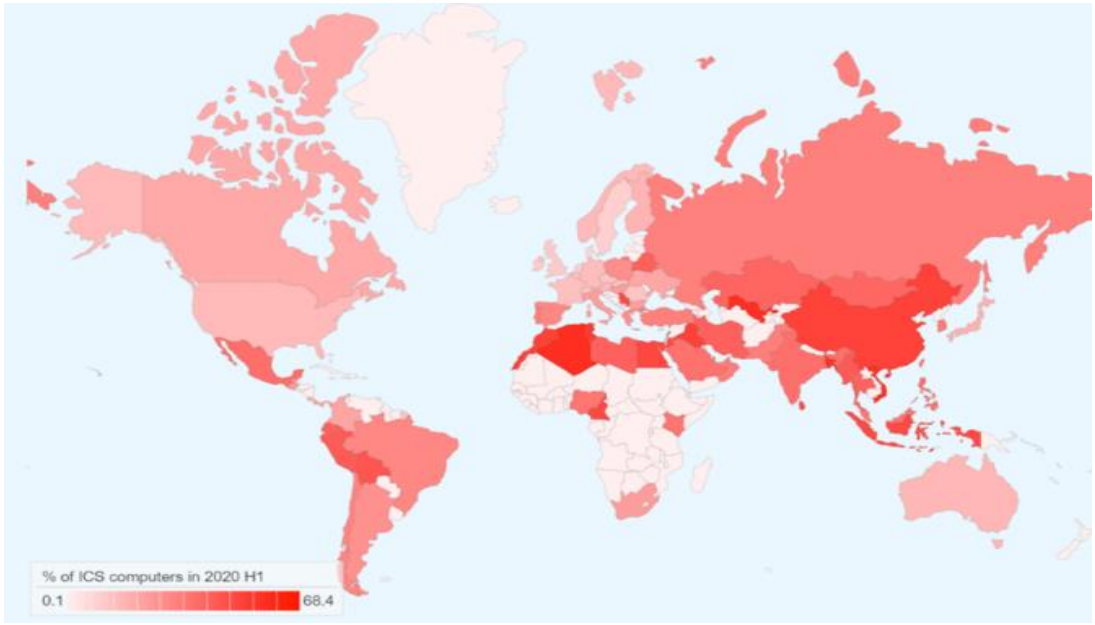
随着工业化和信息化融合的加速，以及工业互联网、智能制造技术的广泛应用，传统 IT 系统面临的网络安全问题同样也在开始向较为封闭的 OT 系统传导。一般而言，OT 系统资产价值较高，安全防护能力弱、漏洞多，正在成为各国黑客攻击的重点。从国别来看，我国一直是全球遭到工控攻击最为严重的地区之一，2020 年上半年中国大陆工控计算机中有超过一半遭受过攻击。

图表16 主要国家和地区工控计算机受攻击比例



资料来源：卡巴斯基工控实验室、平安证券研究所

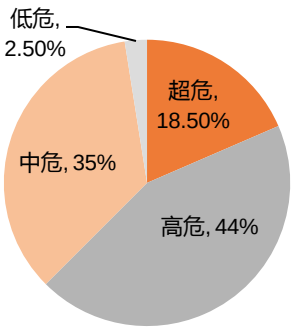
图表17 全球工控计算机受攻击严重程度地图



资料来源：卡巴斯基工控实验室、平安证券研究所

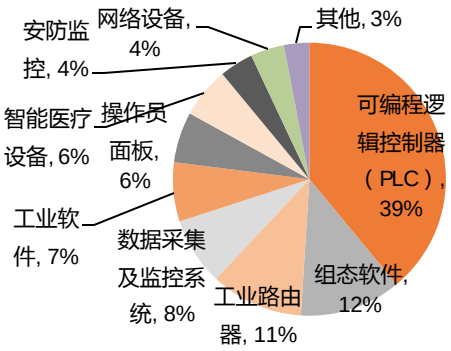
国内工控漏洞众多，影响广泛，潜在风险高。从国家工业信息安全漏洞库收集整理数据显示，2020年工控漏洞数量达到2138个，同比上升22.2%，涉及到335家厂商。在收录的2045个通用型漏洞中，超危漏洞为379个，高危漏洞899个，高危及以上漏洞占比高达62.5%。受影响产品共涉及10个大类、66个小类。其中，工业主机设备和软件类、工业生产控制设备类、工业网络通信设备类分列大类的前三位，可编程逻辑控制器(PLC)、组态软件、工业路由器、数据采集与监控系统(SCADA)、工业软件分列小类的前五位。从厂商来看，德国西门子、法国施耐德、研华科技等公司的产品都受到影响。由于我国在OT领域底层技术方面自主可控程度较低，对漏洞的自主封堵能力较弱，需要依靠原厂能力进行，从发现到封堵的周期很长，漏洞被利用的风险非常高。

图表18 2020 年国内通用型漏洞按危害等级划分情况



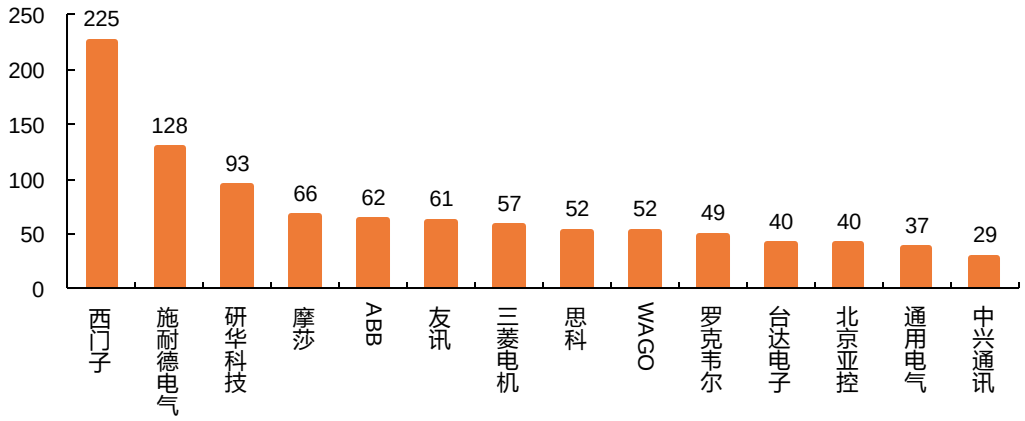
资料来源:国家工业信息安全漏洞库、平安证券研究所

图表19 2020 年国内通用漏洞按照影响行业小类情况



资料来源: 国家工业信息安全漏洞库、平安证券研究所

图表20 2020 年国内通用型漏洞按受影响产品厂商分布情况（个）



资料来源：国家工业信息安全漏洞库、平安证券研究所

国内工业互联网（工控）安全是伴随着工业互联网平台的示范推广发展起来，虽然规模不大，但前景广阔。目前，工业互联网安全处在多种角色共同建设的状态，参与方包括工业企业、平台企业、安全企业、互联网企业、硬件企业等。其中，安全企业作为第三方力量，正在积极参与工控系统的安全体系建设，启明星辰、360 正在将该领域作为战略方向，持续加大投入。安全企业正在利用其在 IT 上积累的安全经验，尝试向 OT 领域输出，提供包括资产测绘、杀毒、防火墙、入侵检测、流量审计等传统安全软件，同时也在尝试利用 SaaS 化的模式为工业互联网平台提供安全技术支撑。

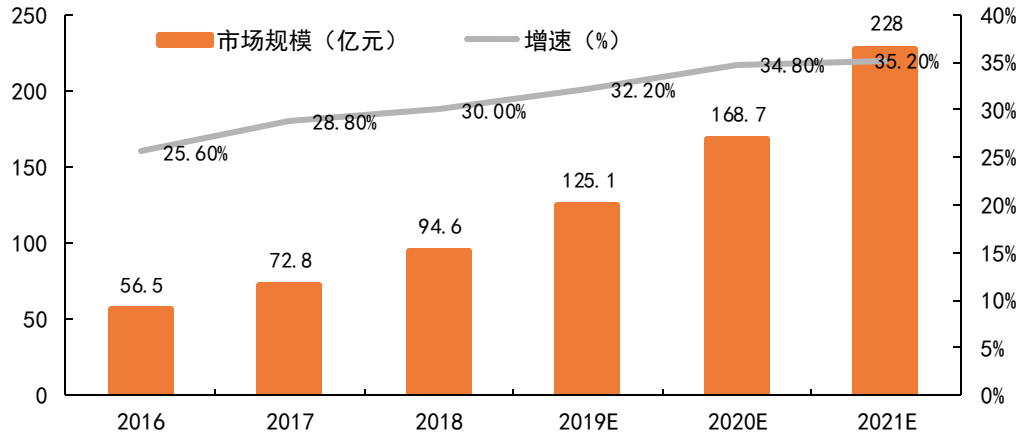
例如，阿里云盾提供了 DDoS 防护、主机入侵防护、Web 应用防火墙、态势感知等一站式安全产品及服务，助力提升工业互联网平台安全防护水平。360、启明星辰等安全厂商为航天云网 Indics 工业互联网平台建立病毒库、漏洞库及防护工具库，支持平台入侵检测、漏洞扫描和主动防御。长扬科技打造了工控安全评估、工控等保检查、工业防火墙、工控主机卫士、统一安全管理、安全态势感知等多种安全产品，支持工业互联网平台安全防护。

图表21 工业互联网平台安全能力薄弱点和侧重点

平台对象	安全能力侧重点	安全能力薄弱点
工业数据	数据加密传输、数据加密存储等	工业数据分类分级、细粒度访问控制、敏感数据识别和保护等
工业应用层	身份认证、权限控制、安全审计等	工业应用安全加固、统一安全运维、应用日志分析等
工业云平台服务层	数据访问控制、安全服务组件、接口安全等	微服务组件安全、工业应用开发环境安全等
工业云基础设施层	抗 DDOS 攻击、访问控制、边界网络安全、云主机杀毒等	虚拟机流量流向可视化，云内网络威胁隔离机制，虚拟化软件安全等
边缘计算层	设备接入认证、网络安全审计、通信加密策略安全防护等	边缘设备可信验证、工业协议深度解析、对接不同厂商端侧设备等

资料来源：工业互联网平台安全白皮书、平安证券研究所

图表22 我国工业互联网安全市场规模及预测



资料来源:赛迪顾问、平安证券研究所

安全服务市场重视程度快速提升，新冠疫情带来新的发展机遇

网络安全的本质，是“人与人的对抗”。然而，在高对抗的背景下，传统网络安全产品——静态“盒子”，已经难以满足客户需求。在这种背景下，安全服务的作用就显现出来。安全服务就是在面对各种威胁时，通过专业人员、技术专家，直面客户诉求，解决客户问题，它是“人与技术”的融合。

国际市场上，安全服务市场已非常成熟，服务收入占整个网络安全产业的比重超过 60%。而在国内市场上，由于安全产品在现有预算体系下更容易核算，加上政企对安全的态度还是以合规为主，提升主动防御能力的组织机构很少，服务预算很少或者根本不重视，造成安全服务占行业市场规模的比重持续低于国际水平，一直以来给人的印象是国内的安全“重硬轻软弱服务”，服务一直是销售安全硬件产品的“赠品”。但近年来，安全服务市场动力不足的状况正在改观，技术专家提供的安全服务的价值正在凸显，政企客户日趋依赖网络安全服务商提供专业的安全集成、安全运维、安全咨询、安全教育与培训等服务，以及时应对各种潜在的、突发的网络安全事件，保障业务健康稳定运行。

疫情以来，虽然给安全服务的开展带来了严峻挑战，但是也带来了巨大的机遇。一方面，云上会议、线上办公大幅改变了客户的用网习惯，对安全服务的认知在提升，中小企业自身安全服务能力较弱，但难以支付高昂的网络安全团队的成本，就开始在市场上寻找成本更低的安全专业化服务，网络安全服务市场上升空间巨大，网络安全服务模式的发展处于历史性机遇期。二是由于企业的全面数字化转型，安全风险面扩大，市场呼唤网络安全服务模式转型。新基建和数字经济战略加速的大背景

下，万物互联，使得数字设备接口、节点指数级上升，网络安全风险暴露面扩大，触点增多，网络安全风险监测、评估、应急处置量急剧上升。以现有网络安全能力，传统的上门装配安全产品、现场终端检测方式根本无法满足需求，市场也在迫切期待网安服务的新业态、新技术、新模式产生。

其中，安全运营中心就是服务新模式的典型。除少数大型企业自建安全运营体系或以线下模式整体外包安全运营服务外，未来主要发展基于云模式的网络安全公共服务平台，将用户设备联网到安全运营中心平台，适时采集安全监测数据，形成全天候 24 小时持续安全监测、检测、防护、应急响应和恢复处置的闭环能力体系，提供远程实时在线的漏洞发现、网站防护、抗拒绝服务攻击、域名安全等服务，打破时间、地域限制，降低供需两侧安全成本。由于高质量、低成本的远程运营中心和运营即服务的应用，将使网络安全产业生态发生重大变化，重塑产业格局、重组安全企业。

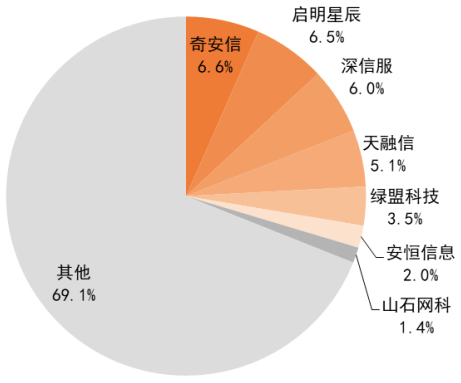
传统安全企业转型案例之启明星辰：发力工业互联网安全、安全运营，培育新的战略优势

启明星辰公司成立于 1996 年，历经二十多年的发展，已成长为国内网络安全行业龙头企业。多年来，启明星辰一直在为企业级用户提供网络安全软硬件产品、可信安全管理平台、安全服务与解决方案。公司的客户覆盖了政府、军队、电信、金融、制造业、能源、交通、传媒、教育等多个行业领域，网络安全产品横跨防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域。

根据中国网络安全产业联盟联合数说安全发布的《2020 年中国网络安全产业分析报告》数据显示，2019 年启明星辰以 6.5%的市场份额排国内网络安全行业的第二位。另据 CCID 数据显示，在传统网络安全产品市场上，启明星辰入侵检测与防御（IDS/IPS）产品市场份额连续 18 年排名第一，统一威胁管理（UTM）产品市场份额连续 13 年排名第一。

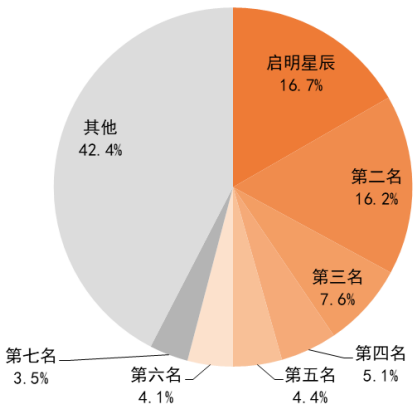
作为国内网络安全行业龙头企业，启明星辰顺应网络安全行业新的发展趋势，在保持传统网络安全产品市场领先地位的同时，积极向工业互联网安全、安全运营等新场景、新服务模式拓展。工业互联网安全和安全运营也成为了启明星辰战略新业务的重要组成部分。

图表23　2019 年我国网络安全市场结构



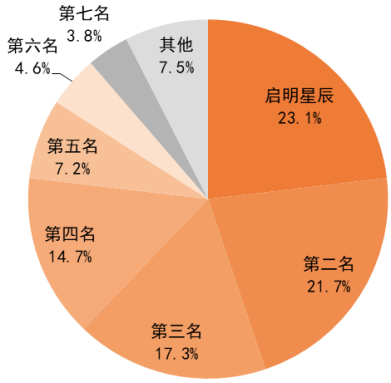
资料来源:《2020 年中国网络安全产业分析报告》、平安证券研究所

图表24　2019 年我国 IDS/IPS 产品市场结构



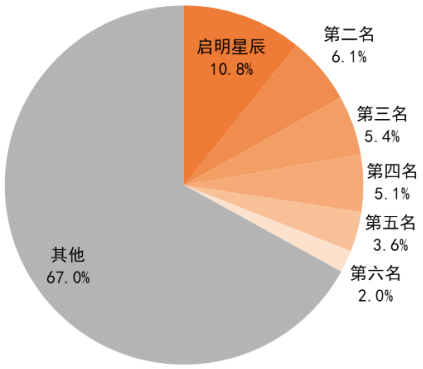
资料来源:CCID、启明星辰公司网站、平安证券研究所

图表25 2019 年我国 UTM 产品市场结构



资料来源:CCID、启明星辰公司网站、平安证券研究所

图表26 2019 年我国数据安全产品市场结构



资料来源:CCID、启明星辰公司网站、平安证券研究所

➢ **工业互联网（工控）安全**

启明星辰的工业互联网安全业务是从工业控制系统安全业务发展而来。启明星辰是国内开展工控系统安全业务最早的安全厂商之一。2014 年，启明星辰参与发起成立了“工业控制系统信息安全产业联盟”。此后，启明星辰基于工业控制系统的安全防护理念，专门研发了工业控制系统安全隔离网闸、工业控制系统防火墙、无线入侵防御系统、工控终端安全管理系统等产品，并从安全防护、安全加固、安全监控、安全运维四个维度，提出了工业控制系统安全解决方案。

当前，启明星辰工业互联网安全业务已形成比较完整的产品体系，产品包括工业防火墙、网络流秩序分析、工控 IDS 与审计、工控脆弱性扫描、工业 SOC、工业网闸、工控检查工具箱、工业主机防护系统、工控态势感知、安全数据交换系统和数据交换总线等产品类。2019 年，启明星辰与行业用户深度合作，落地多个行业级大型工控网络安全项目。根据启明星辰公司公告，2019 年，启明星辰工业互联网安全业务实现收入达到 2 亿元，该板块发展已经形成规模。2020 年上半年，启明星辰持续在行业场景深化上下功夫，推动网络安全与用户业务场景的进一步融合共建，在新技术、新方向上持续投入和发力。我们预计，工业互联网安全业务将成为公司业绩新的增长点。

➢ **安全运营业务**

由于看到安全服务市场的巨大潜力，启明星辰将其作为战略转型方向，其发力点就是城市安全运营中心。智慧城市安全运营中心业务是启明星辰专门为智慧城市信息化建设和运行配套打造的一揽子高端安全服务，为智慧城市的安全运转保驾护航。此项业务开启新的安全服务市场和新的利润模式。

2017 年 12 月，启明星辰开启了国内首个智慧城市安全运营中心——成都安全运营中心，面向四川省提供智慧城市数据与安全运维服务。2018 年，启明星辰与天津市合作，建设覆盖京津冀的区域性总部，成立辐射京津冀的启明星辰安全监控预警中心与安全服务应急响应中心；同年，公司与青岛市合作，建设环黄海区域网络安全运营中心。

为进一步加快安全运营业务的发展，快速抓住市场先机，启明星辰于 2017 年公告发行可转换公司债券预案，拟通过发行可转换公司债券募集资金总额不超过 10.9 亿元。扣除发行费用后，募集资金将投资于“济南安全运营中心建设项目”、“杭州安全运营中心建设项目”、“昆明安全运营中心和网络培训学院建设项目”、“郑州安全运营中心和网络培训学院建设项目”和“补充流动资金”等五个项目。2019 年，启明星辰完成本次可转债发行，发行可转债总额为 10.45 亿元。

据公司公告称，2019年，启明星辰安全运营体系已基本形成北京、成都、广州、杭州（东西南北）四大业务支撑中心及30余个城市运营中心，已形成成熟的标准化运营体系，并持续向其他二三级城市拓展。根据启明星辰公司公告，2019年，启明星辰安全运营业务实现收入3.5亿元。

图表27 启明星辰可转债募投项目

项目名称	项目总投资额（万元）	拟投入募集资金（万元）	自筹资金投入额（万元）
济南安全运营中心建设项目	9200	5700	3500
杭州安全运营中心建设项目	28000	13500	14500
昆明安全运营中心和网络安全培训中心建设项目	47300	37300	10000
郑州安全运营中心和网络安全培训中心建设项目	50500	33000	17500
补充流动资金	15000	15000	-
合计	**150000**	**104500**	**45500**

资料来源：启明星辰公司公告、平安证券研究所

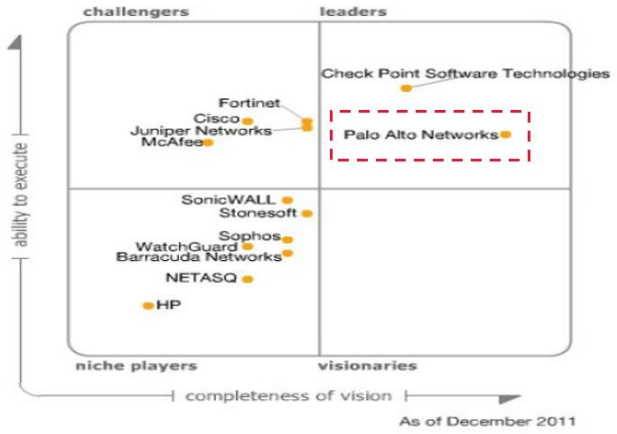
三、 云安全等新赛道在国际市场上已得到成功验证，国内转型适逢其时

相较而言，国内网络安全还在起步阶段，安全投入和技术同国际先进水平还有较大差距。从新技术应用程度和发展阶段角度看，国内还处在追赶状态，因此国际龙头安全企业的发展路径，也可以供国内安全企业参考。近年来，在国际市场上，传统安全企业如Palo Alto Networks、Fortinet等均在向云安全、数据安全市场转型，并取得了积极效果。同时，在美国市场涌现出来的一些专业企业如Zscaler、Crowdstrike等，在云安全、终端安全等方面均形成了独特的竞争力，并持续受到市场的热捧。国际市场上，传统企业转型成功以及新兴企业的崛起，证明了走“新安全”这条路是可行的。国内无论是新安全企业继续拓展还是传统企业向该领域转型，成功几率均较高。

3.1 Palo Alto：综合安全能力全球领先，积极通过并购等手段向新方向转型

Palo Alto是全球领先的网络安全公司，2005年成立，2012年在纽交所上市。公司从防火墙业务起家，快速发展成为具备综合防护能力的安全企业。2007年，公司发布了首款企业下一代防火墙，相比传统防火墙产品，下一代防火墙较好的融合了传统防火墙和应用防护的能力，曾经掀起了一轮防火墙技术的变革。凭借着该领域的先发优势，短短几年公司的下一代防火墙产品就进入了Gartner企业防火墙魔力象限（2011年），此后一直处于行业的领导者地位，且领先地位较为稳固。据公司官网数据显示，财富100强企业中有85%使用了公司产品，总客户数量超过65000家。

图表28 2011 年 Gartner 全球企业防火墙魔力象限



资料来源：Gartner、平安证券研究所

图表29 2020 年 Gartner 全球企业防火墙魔力象限

资料来源: Gartner、平安证券研究所

防火墙领域的成功使得 Palo Alto 在安全市场上站稳了脚跟，此后就开始丰富其产品线，力图为客户提供完整的企业安全解决方案。目前，公司形成了三大业务体系，包括企业安全（STRATA）、云安全（PRISMA）和安全运营（CORTEX）。其中，企业安全主要是智能网络安全解决方案，包括基于人工智能（机器学习）的下一代防火墙，交付形式包括物理防火墙、虚拟防火墙以及云上交付的防火墙；公司的云安全平台是业界领先的原生安全平台，可以对云上应用、数据和环境进行有效保护，适用于多云和混合云场景；安全运营（面向未来的安全）主要是终端安全 XDR、XSOAR（安全工具的自动化编排和响应），此外还有威胁情报 AutoFocus 和安全数据湖，此类产品也在通过软件和 SaaS 等灵活模式交付。

图表30 Palo Alto 主要业务板块

资料来源:公司网站、平安证券研究所

公司自 2017 年以来，产品线拓展显著加速，主要走的两条路。一是内部研发，包括防火墙、云计算以及安全运营等产品线的持续升级。另一方面，持续收购安全创新企业，快速补齐业务短板，收购涉及的领域包括云安全、数据安全和物联网安全等。2019 年，公司在云安全领域大手笔发力，连续

收购了三家云安全企业，包括 Puresec、Twistlock、Aporeto；2020 年，除了云安全之外，公司在主动防御（攻击面管理）、终端安全等方面更是出手频频，业务板块趋于完整。

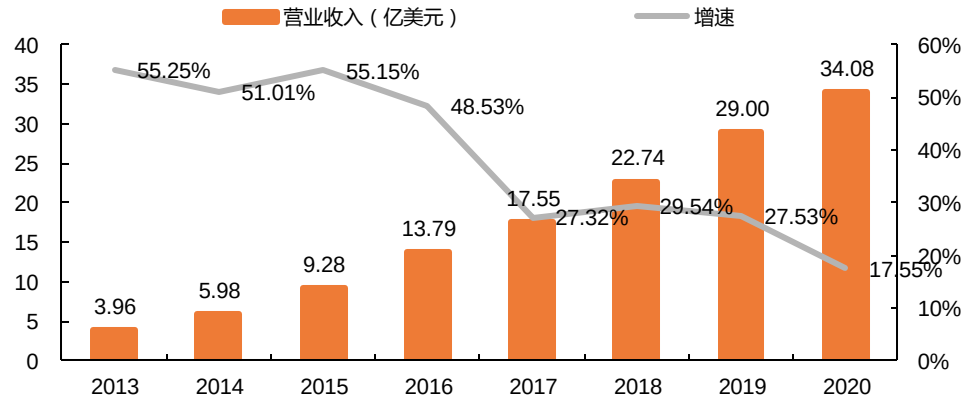
图表31 2017 年以来公司主要收购情况

收购标的	主要业务	收购时间
LightCyber	以色列安全检测平台企业	2017 年
Secdo	以色列知名终端安全企业，公司在数据采集和可视化方面有着独到的竞争力，可以利用收集的数据进行更高精准度的检测、可视和阻断，可以大幅度提升安全运维响应时间	2018 年
vident.io	云安全企业，业务重点是云安全和合规自动化，其 Evident Security Platform 监控云部署，评估风险并提供补救指导	2018 年
Redlock	云安全分析、高级威胁检测和合规性监测	2018 年
Demisto	以色列数据安全公司，业务侧重于安全工具编排和自动化安全技术	2019 年
Puresec	美国云安全公司，主要产品为可信的安全计算环境中构建和维护安全可靠的无服务器应用	2019 年
Twistlock	技术领先的容器安全企业	2019 年
Zingbox	物联网安全创业公司	2019 年
Aporeto	云安全创业公司，在分布式防火墙、身份识别代理和特权访问管理的产品方面有着比较强的竞争力	2019 年
CloudGenix	全球领先的云交付厂商	2020 年
Crypsis Group	终端安全企业，专注于事件响应、风险管理和数字取证	2020 年
Expanse	攻击面管理的安全初创公司，扫描企业 IT 资产提供漏洞监控服务	2020 年
Sinefa	公司主要提供网络流量、终端监测等解决方案	2020 年

资料来源：公司网站、平安证券研究所

公司云安全和安全运营的拓展非常成功，订阅收入和服务增长快于产品，占比持续扩大。云安全和安全运营在收入上主要体现为订阅和服务收入。我们看到，即使 2020 年产品收入微跌的背景下，公司的订阅和服务收入依然保持着较快增长。2020 财年，公司实现收入 34.08 亿美元，同比增长 17.55%。其中，产品收入由于市场渗透率提升，竞争趋于激烈，造成部分价格下调，收入略有下降；但是订阅和服务收入增长很快，分别增长 36.1%和 21.8%，占收入比重分别为 41.23%和 27.55%，其订阅收入在 2018 财年之后占比持续扩大，是其云转型成功的重要体现。

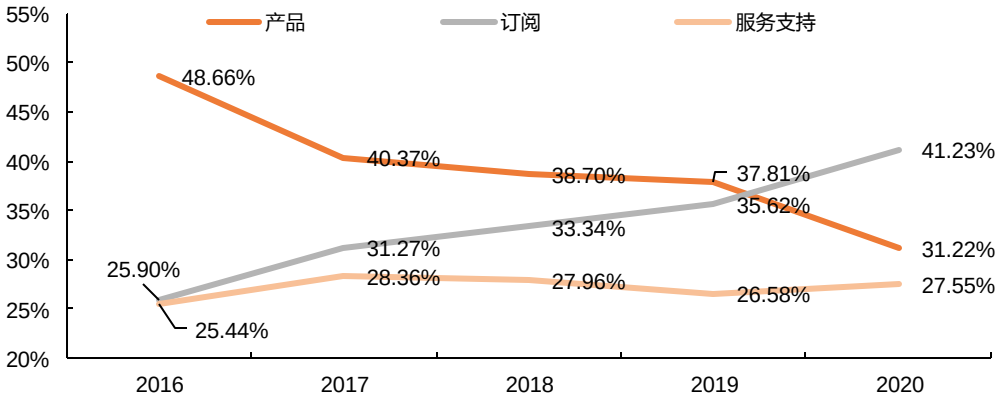
图表32 Palo Alto公司各财年营业收入及同比增速



资料来源:公司年报、平安证券研究所

注：公司各财年截至日期为7月31日，下同。

图表33 Palo Alto公司各财年收入构成情况



资料来源:公司年报、平安证券研究所

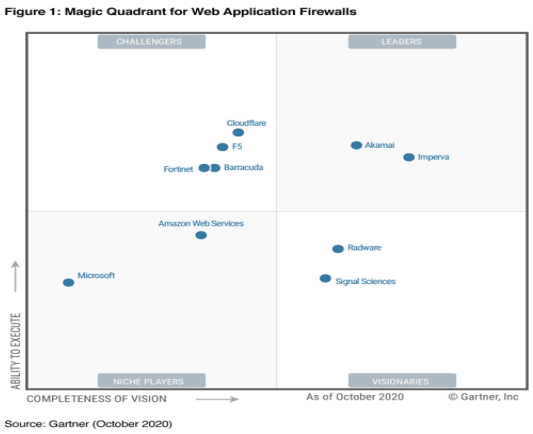
3.2 Fortinet：安全能力云化转型成功，AI在安全产品和服务方案中应用广泛

Fortinet（中文名：飞塔公司）是全球知名的企业安全提供商，公司在网络安全、基础设施安全、云安全、终端及物联网安全等方面都有着较强的竞争能力，客户超过45万户，覆盖了大型企业、服务提供商和政府机构。据Gartner行业魔力象限显示，公司网络防火墙持续多年处于领导者地位；Web应用防火墙（Web Application Firewall，简称WAF）魔力象限中处在挑战者地位；网络基础设施（含有线和无线）在魔力象限中处在远见者地位，未来可能有进入领导者象限的潜力。

公司网络安全产品包括下一代防火墙、安全订阅服务、安全情报分析及响应等。该部分收入主要来自于网络安全设备——FortiGate，应用覆盖了内网及边界安全，包括防火墙、安全网关、SD-WAN、IPS、SSL数据泄露防护、VPN等。公司是典型的平台化企业，其网络安全产品及基础设施都可以通过FortiOS进行管理。基础设施安全业务涵盖了除了网络安全之外的基础设施安全防护能力，包括Wi-Fi和交换机。公司云安全产品可以帮助客户安全连接他们的公有云、私有云或者混合云，产

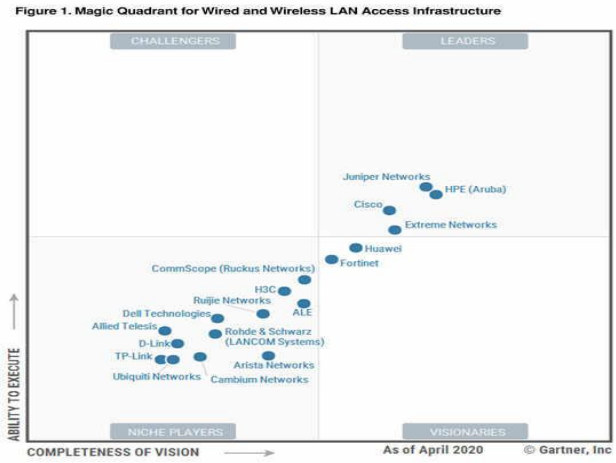
品和服务都可以通过公有云、私有云或者软件交付的形式获得，公有云合作伙伴包括 AWS、Azure、Google Cloud、Oracle Cloud、阿里云等。

图表34 2020 年 Gartner 全球 WAF 魔力象限



资料来源：Gartner、平安证券研究所

图表35 2020 年 Gartner 网络基础设施魔力象限

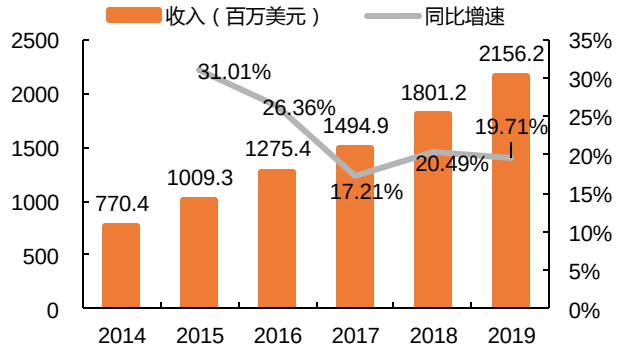


资料来源: Gartner、平安证券研究所

Fortinet 主要是通过渠道进行产品和服务的销售，采取的是两级分销的模式，在特定情况下公司才会直接面对大型服务提供商和主要的系统集成商。同时，公司也会通过前述的云运营商合作伙伴销售产品，客户可以在合作伙伴的平台上购买 License 并使用；此外，客户也可以购买授权将软件部署在自己的私有云平台上使用。

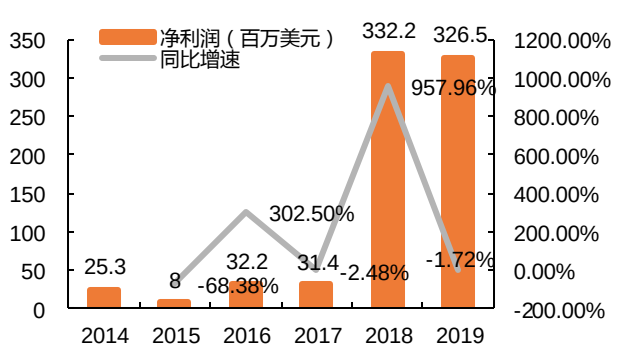
公司产品和服务能力均十分优秀，但是收入主要还是来自于服务，尤其是订阅服务。公司 2019 年 21.56 亿美元的收入中，有 63%是来自于服务收入，而且占比较为稳定。公司服务业务主要来自于两块，一是 FortiGuard 安全订阅收入，另一个就是 FortiCare 的 IT 技术服务。FortiGuard 安全订阅服务是由公司 FortiGuard Lab 提供，可选功能包括入侵检测、Web 过滤、反病毒、反垃圾邮件、数据库安全、安全评级服务等。FortiGuard 平台在应对当前快速变化的网络安全环境中的优势明显，所有应用可以快速实现交付。2019 年，公司服务收入增长 21%，其中 FortiGuard 安全订阅服务收入增长 24%。另外，云订阅模式的收入指标——递延收入，增长也较为迅速。2019 年公司递延收入为 21.35 亿美元，同比增长 26.6%，明显快于公司收入增速，可见公司正在从云安全的发展中受益。

图表36 2014-2019 年 Fortinet 收入及同比增长



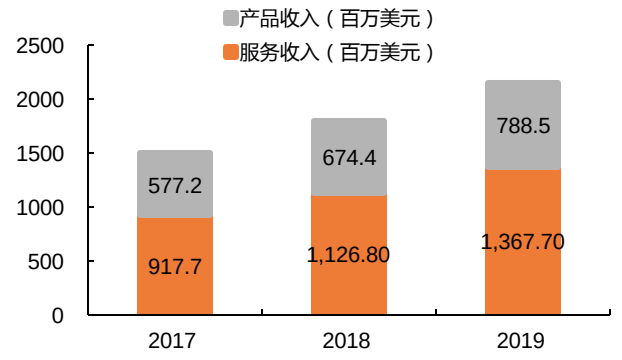
资料来源：公司年报、平安证券研究所

图表37 2014-2019 年 Fortinet 净利润及同比增速



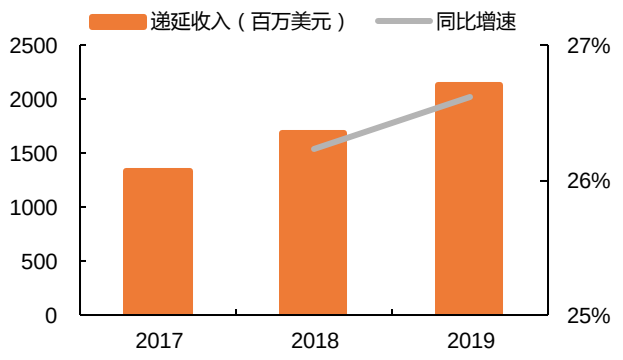
资料来源: 公司年报、平安证券研究所

图表38 2017-2019 年 Fortinet 产品及服务收入



资料来源：公司年报、平安证券研究所

图表39 2017-2019 年 Fortinet 递延收入及同比增速



资料来源：公司年报、平安证券研究所

Fortinet 为实现加速向云安全厂商转型，和 Palo Alto 类似，也开展了多次并购。公司和云安全相关的最早的一次并购发生在 2018 年 11 月，公司收购了 ZoneFox Limited，一家位于苏格兰的企业，主要提供基于云端的内部威胁检测和响应解决方案，而且后者基于机器学习的威胁搜索与查杀技术的集成对 Fortinet 现有的安全解决方案是一个很好的补充。2020 年 7 月，公司收购了云安全和网络创新企业 OPAQ Networks，后者的零信任云解决方案可为组织提供从数据中心到分支机构再到远程用户和物联网（IoT）设备的分布式网络提供强大保护。2020 年 12 月，Fortinet 收购了网络安全公司 Panopta，后者的 SaaS 平台可以为混合环境（包括边缘和云网络）提供更好的网络可视性和快速补救，此次收购可以帮助 Fortinet 提升现有产品效率。

除了云安全之外，Fortinet 也越来越关注人工智能技术的应用。近年来，安全行业开始重视对威胁情报的分析，以用于主动防御，但是由于业主采用的安全设备来源五花八门、事件告警多但有效告警少、手动反应慢而且缺乏专业的人手，威胁情报利用效率非常低。很多公司开始尝试利用人工智能进行安全威胁情报的分析，Fortinet 就是应用比较成功的一家企业。除了关联日志文件或执行设备修补和更新等常规应用之外，公司还将机器学习系统融入到其产品和服务中，将客户的 IT 部门和安全基础设施提供的海量信息进行汇总、分析和丰富，并发出威胁警报，提供自动编排和响应手段，自动阻止、检测和响应网络威胁，使得整个用户网络管理变得更为高效、简单。

3.3 CrowdStrike：云原生安全服务商，在终端安全市场全球领先

CrowdStrike 公司成立于 2011 年，已于 2019 年在美国纳斯达克交易所上市。公司致力于重塑云时代的安全性，构建了 Falcon（猎鹰）平台来检测网络安全威胁并阻止漏洞。公司借助 Falcon 平台，创建了多租客、云原生的智能安全解决方案，能够为运行在各种终端（例如笔记本、台式机、服务器、虚拟机、物联网设备）的本地部署的、虚拟化的以及基于云的工作场景提供网络安全保护。公司的智能安全解决方案能够应对复杂攻击，保护客户数据安全。

公司的 Falcon 平台由两项紧密集成的自有技术组成：易于部署的智能轻量级代理和基于云的动态图形数据库——威胁图。这两种紧密集成的自有技术通过使用 AI 技术和模式匹配技术相结合，在整个网络安全威胁生命周期持续收集、处理、分析和关联大量的高保真数据来阻止违规行为。公司通过在整个客户群众包数据并利用规模经济来实施这种方法。公司认为，这样会使公司的 AI 算法具有独特的效果。公司基于云的 AI 技术也会与社区中的每一个客户实时共享。在整个网络安全威胁生命周期中，公司综合使用了多种针对已知的和未知的网络安全威胁以及恶意软件和非恶意软件技术的方法。

图表40 CrowdStrike 公司 Falcon 平台技术特点

云原生架构	公司完全面向云环境构建了猎鹰平台，从而能够收集和分析来自所有客户的大量众包数据以阻止违规行为
Falcon 代理	公司设计了一个智能轻量级代理，该代理安装在每个终端上。这些代理结合了对已知恶意软件的识别和预防、对未知恶意软件的机器学习、利用漏洞阻止和高级行为技术，可在捕获和记录高保真终端数据的同时保护所有终端的工作负载
威胁图	威胁图是一个公司自有的、功能强大的动态图形数据库。威胁图通过将 AI 与行为模式匹配技术相结合分辨文件特征并跟踪客户网络环境中在终端上执行的每个应用程序的行为，来不断寻找恶意活动
高保真数据和智能过滤	智能过滤能够将客户终端上的开销降至最低，大幅减少 Falcon 代理与云通信的带宽，有效处理大量数据，并将信号和噪音分离
管理界面	Falcon 平台管理界面为客户提供了他们整个环境的直观信息，并具有及时的警报和详细的搜索功能
API 和集成	Falcon 平台和体系架构是围绕一组丰富的 API 构建的，这些 API 可以有效补充和扩展客户现有的安全基础架构，例如安全信息事件管理、SIEMs、入侵防御系统和入侵检测系统

资料来源:CrowdStrike 公司公告、平安证券研究所

Falcon 平台通过基于 SaaS 订阅的模型集成了 11 个模块，该模型横跨多个大型安全市场。当前，Falcon 平台的云模块涵盖了终端安全、安全和 IT 运营（包括漏洞管理）、威胁情报等类别，面向终端安全、威胁情报、安全和漏洞管理、IT 服务管理软件和托管安全服务等五个市场。

图表41 CrowdStrike 公司 Falcon 平台市场和产品简介

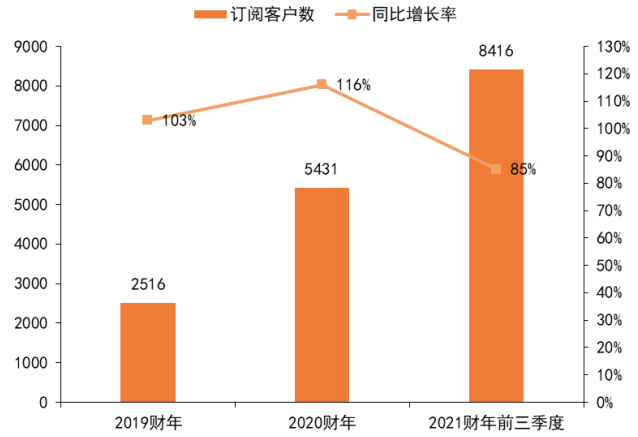
终端安全	➢ 2013 年，公司推出 EDR（终端检测与响应）产品 Falcon Insight 云模块 ➢ 2017 年，公司推出下一代防病毒软件 Falcon Prevent ➢ 根据 IDC 预估，EDR 和下一代防病毒市场有望在 2021 年达到 87 亿美元
威胁情报	➢ 2012 年，公司推出威胁情报产品 Falcon X 云模块 ➢ 根据 IDC 预估，威胁情报市场有望在 2021 年达到 20 亿美元
安全和漏洞管理	➢ 2017 年，公司推出安全和漏洞管理产品 Falcon Spotlight ➢ 根据 IDC 预估，安全和漏洞管理市场有望在 2021 年达到 104 亿美元
IT 服务管理软件	➢ 2017 年，公司推出 IT 服务管理软件产品 Falcon Discover ➢ 根据 IDC 预估，这一细分市场有望在 2021 年达到 20 亿美元
托管安全服务	➢ 2018 年，公司推出托管安全服务产品 Falcon Complete ➢ 根据 IDC 预估，这一细分市场有望在 2021 年达到 296 亿美元。公司预计公司在这一细分市场的潜在市场机会在 2021 年将达到 51 亿美元

资料来源:CrowdStrike 公司公告、平安证券研究所

公司在美国和德国都设有数据中心托管设施，同时公司也使用位于美国的 AWS 数据中心来满足存储需求并协助交付公司的解决方案。公司的技术架构与选用的 AWS 资源相结合，为公司提供了全球范围的分布式可扩展架构。公司为全球客户提供终端安全、安全和 IT 运营、威胁情报等网络安全订阅服务，客户包括财富 100 强企业、全球 100 强企业和排名前 20 的银行等大型企业客户。截至 2020

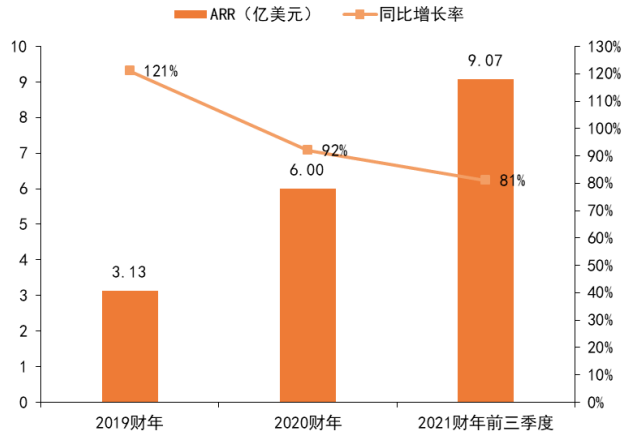
年 10 月 31 日，公司订阅客户增长至 8416 家，同比增长 85%；ARR（年度经常性收入）为 9.07 亿美元，同比增长 81%。

图表42 CrowdStrike 公司 2019 财年至 2021 财年前三季度订阅客户数迅速增长



资料来源:CrowdStrike 公司公告、平安证券研究所

图表43 CrowdStrike 公司 2019 财年至 2021 财年前三季度 ARR 迅速增长



资料来源:CrowdStrike 公告公告、平安证券研究所

CrowdStrike 在全球终端安全市场处于领先地位。凭借基于云的新一代的网络安全产品和技术在客户群体中的迅速拓展，CrowdStrike 在全球终端安全市场快速取得领先地位。CrowdStrike 在 2019 年 Gartner 终端保护平台魔力象限中被评为领导者，并且在整个魔力象限的愿景完整性方面领先于其他厂商。

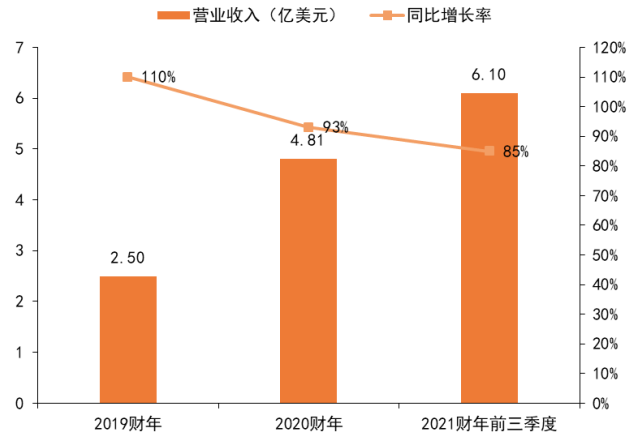
图表44 CrowdStrike 在全球终端安全市场处于领先地位

资料来源:Gartner、平安证券研究所

公司营收持续高增长。公司 2019 财年（2018 年 2 月至 2019 年 1 月）、2020 财年和 2021 财年前三季度营业收入分别为 2.50 亿美元、4.81 亿美元、6.10 亿美元，同比分别增长 110%、93%、85%。

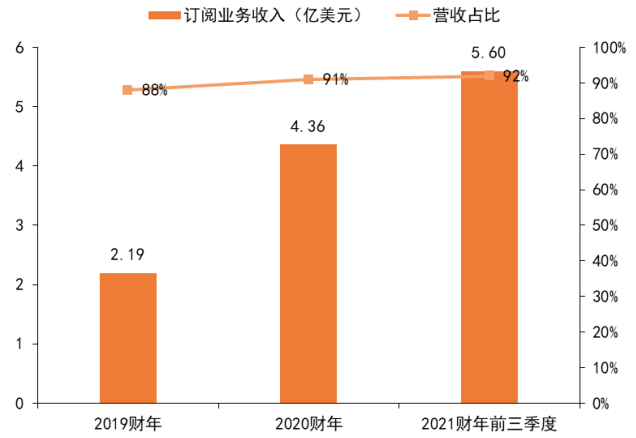
其中，订阅业务收入占比分别为 88%、91%、92%。公司自 2017 财年以来营收持续高速增长，2017 财年至 2020 财年营收年均复合增长率高达 109%，大幅高于同期全球网络安全行业增速。

图表45 CrowdStrike 公司营收持续高速增长



资料来源:CrowdStrke 公司公告、平安证券研究所

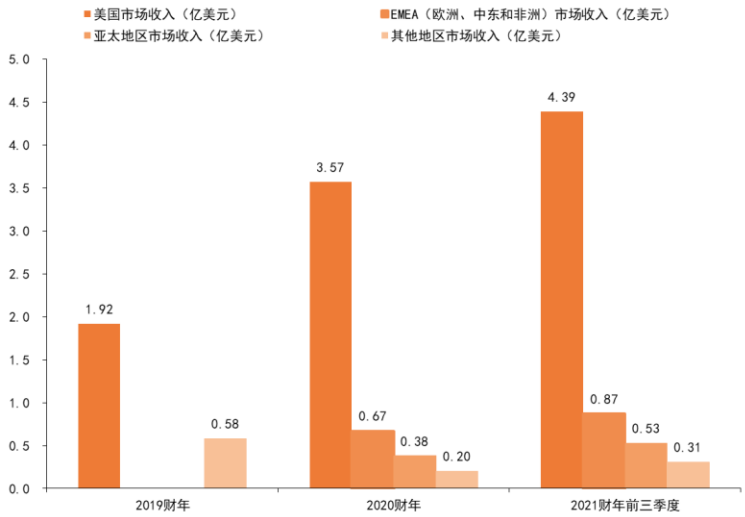
图表46 CrowdStrike 公司订阅业务营收占比持续提高



资料来源:CrowdStrike 公司公告、平安证券研究所

公司的收入主要来自美国市场。公司 2019 财年、2020 财年和 2021 财年前三季度美国市场收入分别为 1.92 亿美元、3.57 亿美元和 4.39 亿美元，占公司营收的比例为 77%、74%、72%。

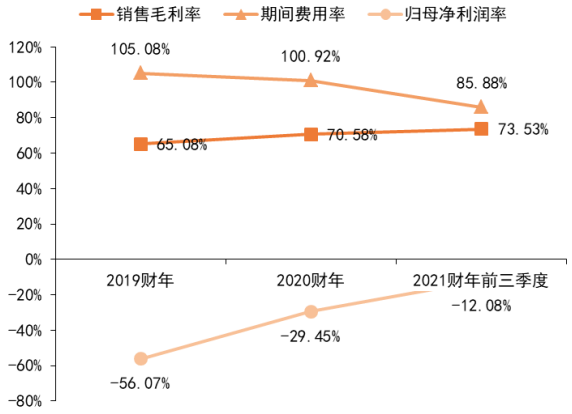
图表47 CrowdStrike 公司的收入主要来自美国市场



资料来源:CrowdStrike 公司公告、平安证券研究所

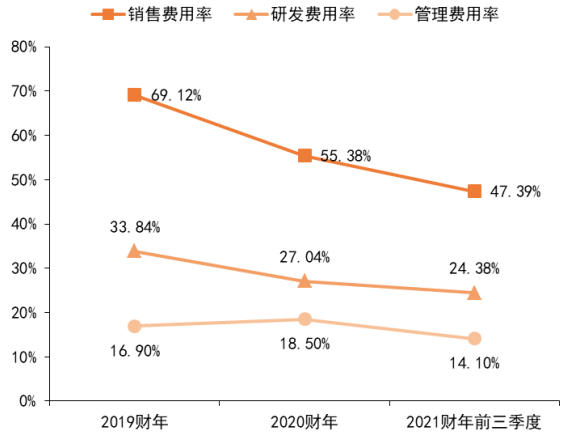
公司毛利率水平较高，且呈现上升趋势。公司 2019 财年、2020 财年和 2021 财年前三季度毛利率分别为 65.08%、70.58%、73.53%。由于员工人数的持续增长，公司的营业费用率也一直保持在较高水平，但呈现下降趋势。公司 2019 财年、2020 财年和 2021 财年前三季度营业费用率分别为 105.08%、100.92%、85.88%。因为公司营业费用率高于毛利率，公司当前仍处于亏损状态，但归母净利润率已经在持续提高。

图表48 CrowdStrike 公司毛利率、营业费用率、归母净利润率分析



资料来源:CrowdStrke 公司公告、平安证券研究所

图表49 CrowdStrike 公司销售费用率、研发费用率、管理费用率分析

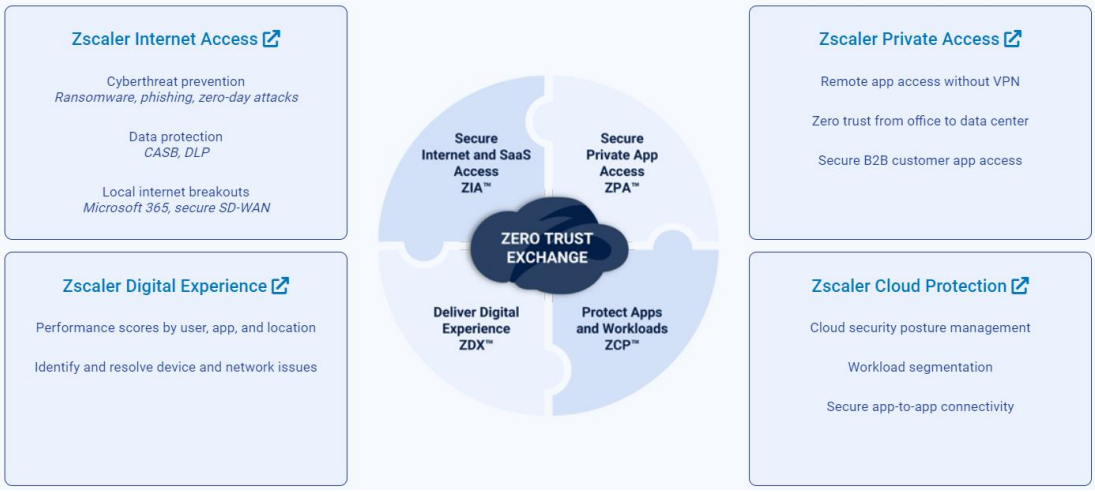


资料来源:CrowdStrke 公司公告、平安证券研究所

3.4 Zscaler：全球领先的零信任架构云安全服务商

Zscaler 成立于 2007 年，成立之初名为 SafeChannel，2008 年改名为 Zscaler，并于 2018 年在美国纳斯达克交易所上市。Zscaler 致力于为客户提供云上的网络安全服务，在客户的应用正在迅速迁移到云上的情况下，通过零信任交换云安全平台（Zero Trust Exchange cloud security platform）为客户提供云端的安全访问应用程序和数据的服务。Zscaler 的零信任交换云安全平台包括四个云原生的综合解决方案：ZIA（Zscaler Internet Access，Zscaler 互联网访问）、ZPA（Zscaler Private Access，Zscaler 私有应用程序访问）、ZDE（Zscaler Digital Experience，Zscaler 数字化体验）和 ZCP（Zscaler Cloud Protection，Zscaler 云保护）。

图表50 Zscaler 公司零信任交换云安全平台架构



资料来源:Zscaler 公司网站、平安证券研究所

Zscaler 是全球云安全领域零信任架构产品的领先供应商。凭借零信任架构在云安全领域的出色表现，公司连续十年被评为 Gartner 安全 Web 网关魔力象限的领导者，且在 2020 年是领导者象限的唯一

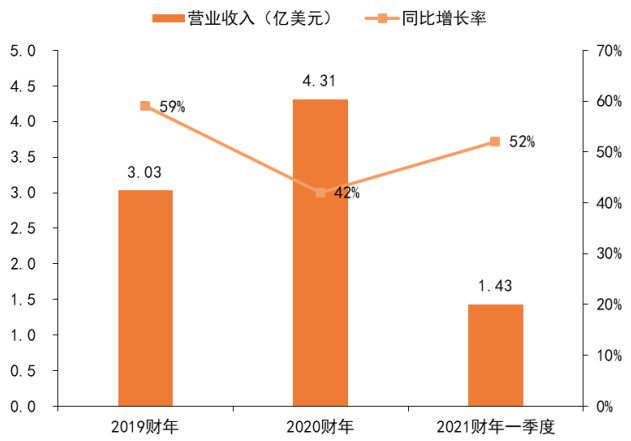
厂商。截至 2020 年 7 月底，Zscaler 的云原生零信任架构分布在全球 150 个数据中心中，为客户提供快速、安全和可靠的访问。Zscaler 云平台每天阻止超过 1 亿个网络安全威胁，并执行超过 175000 个不同的安全更新。Zscaler 客户已超过 4500 家，遍及各个主要行业，包括金融服务、医疗健康、制造业、航空公司和运输、大型企业集团、消费品和零售等。

图表51 Zscaler 是 2020 年 Gartner 安全 Web 网关魔力象限的唯一领导者厂商

资料来源:Zscaler 公司网站、Gartner、平安证券研究所

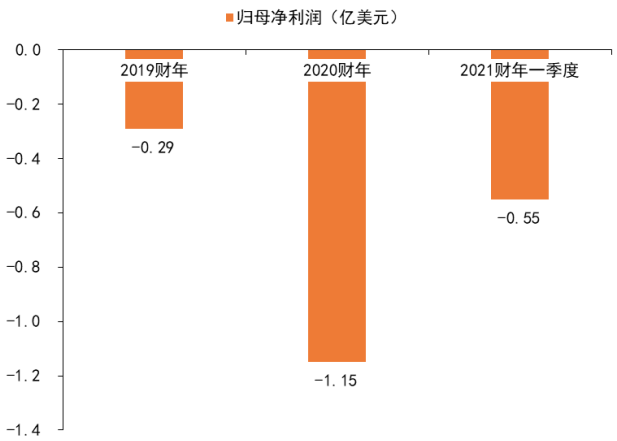
公司营收持续高速增长。公司 2019 财年（2018 年 8 月至 2019 年 7 月）、2020 财年、2021 财年一季度营收分别为 3.03 亿美元、4.31 亿美元、1.43 亿美元，同比增长 59%、42%、52%。其中，订阅和相关支持服务业务的营收占比分别约为 99%、98%、97%。公司营收增长势头良好，但公司自成立以来持续净亏损。根据公司公告，公司预计在可预见的将来将继续净亏损，因为公司将持续增加营销人员并持续加大研发投入。

图表52 Zscaler 公司营收持续高速增长



资料来源:Zscaler 公司公告、平安证券研究所

图表53 Zscaler 公司持续净亏损

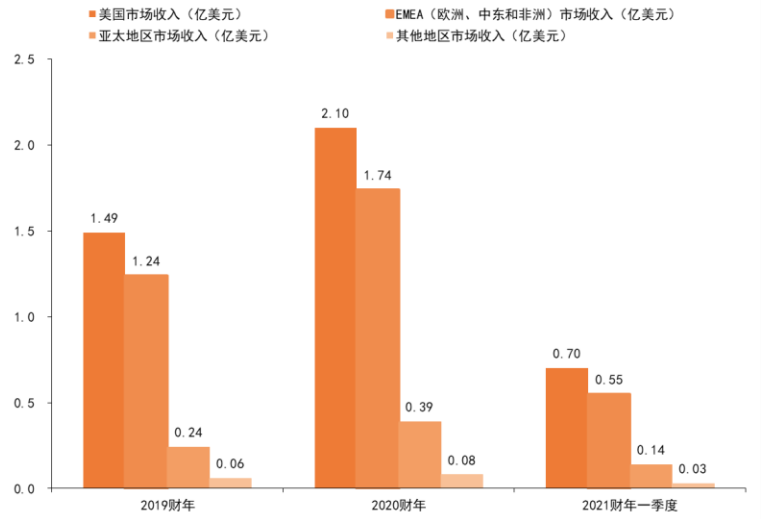


资料来源:Zscaler 公司公告、平安证券研究所

公司的收入主要来自于美国市场和 EMEA（欧洲、中东和非洲）市场。公司 2019 财年、2020 财年和 2021 财年一季度美国市场收入分别为 1.49 亿美元、2.10 亿美元、0.70 亿美元，占公司营收的比

例均为 49%；EMEA 市场收入分别为 1.24 亿美元、1.74 亿美元、0.55 亿美元，占公司营收的比例为 41%、40%、39%。

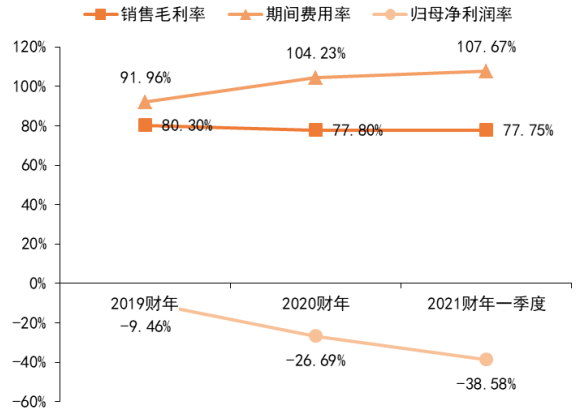
图表54 Zscaler 公司的收入主要来自美国市场和 EMEA 市场



资料来源:Zscaler 公司公告、平安证券研究所

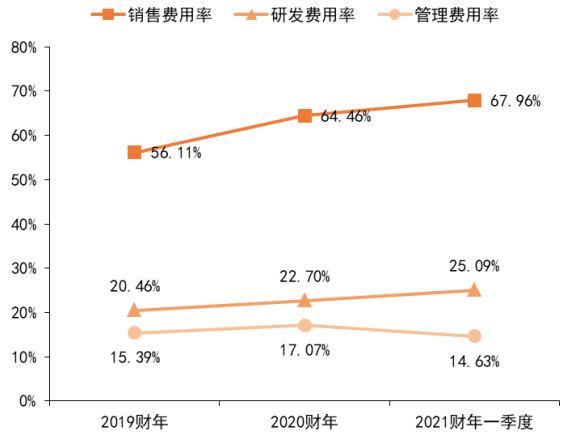
公司毛利率水平较高。公司 2019财年、2020财年和 2021财年一季度毛利率分别为 80.30%、77.80%、77.75%。由于公司持续增加营销人员并持续加大研发投入，因此公司营业费用率持续处于高位。公司 2019 财年、2020 财年和 2021 财年一季度营业费用率分别为 91.96%、104.23%、107.67%。

图表55 Zscaler 公司毛利率、营业费用率、归母净利润率分析



资料来源:Zscalser 公司公告、平安证券研究所

图表56 Zscaler 公司销售费用率、研发费用率、管理费用率分析



资料来源:Zscaler 公司公告、平安证券研究所

四、 投资建议及风险提示

4.1 投资建议

随着数字经济发展的提速，云安全、数据安全将面临着巨大的发展机遇，国内一些新兴安全企业有望实现跨越式发展，传统安全龙头也有望在这一轮洗牌中实现蜕变。云安全板块，推荐深信服，公司是国内私有云解决方案和网络安全的“双料”龙头企业，云和安全的协同性较好，云安全产品具有较强的竞争力。数据安全和工控安全板块，推荐安恒信息，关注奇安信。安恒信息自数据库安全起家，态势感知、AiLPHA 大数据智能安全平台都呈现出良好的增长势头；奇安信在基于大数据的检测控制、分析与监测等安全产品上具有较强的竞争力，而且在工控态势感知平台的建设上也取得了积极进展。

4.2 风险提示

1）竞争加剧的风险。随着新安全市场的发展，不同背景的安全厂商同台竞争的可能性增大，比如互联网、传统 ICT 企业等，技术、品牌、人才和资金等方面的竞争加剧，行业总体和企业毛利率都存在下降的风险。

2）技术风险加剧。新领域的安全防护能力建设需要的是持续的研发投入，我国在新安全领域的研发同国际巨头还存在较大的差距，研发方向选择失误或者研发进度不及预期，都可能对企业短期业绩和长期发展带来不利影响。

3）客户安全支出不及预期。行业客户多采用预算制进行产品和服务采购，宏观经济环境如出现不景气可能影响部分行业客户的 IT 投资预算。2021 年以来，其他国家新冠疫情仍在蔓延，中美经贸关系也存在较大不确定性，国内经济增长仍面临较大压力，公司客户信息安全投入可能被迫下调或者推迟。

平安证券研究所投资评级：

股票投资评级:

强烈推荐 （预计 6 个月内，股价表现强于沪深 300 指数 20%以上）

推　　荐 （预计 6 个月内，股价表现强于沪深 300 指数 10%至 20%之间）

中　　性 （预计 6 个月内，股价表现相对沪深 300 指数在±10%之间）

回　　避 （预计 6 个月内，股价表现弱于沪深 300 指数 10%以上）

行业投资评级:

强于大市 （预计 6 个月内，行业指数表现强于沪深 300 指数 5%以上）

中　　性 （预计 6 个月内，行业指数表现相对沪深 300 指数在±5%之间）

弱于大市 （预计 6 个月内，行业指数表现弱于沪深 300 指数 5%以上）

公司声明及风险提示：

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

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

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

市场有风险，投资需谨慎。

免责条款：

平安证券

平安证券研究所　　电话：4008866338

深圳	上海	北京
深圳市福田区福田街道益田路 5023 号平安金融中心 B 座 25 层 邮编：518033	上海市陆家嘴环路 1333 号平安金融大厦 26 楼 邮编：200120 传真：（021）33830395	北京市西城区金融大街甲 9 号金融街中心北楼 15 层 邮编：100033