东兴证券 DONGXING SECURITIES

信息安全：中美云安全产业对比研究，国内云安全公司空间几何？

——信息安全行业专题报告之二

2020 年 06 月 29 日

看好/维持

计算机 | 行业报告

分析师	王健辉 电话：010-66554035 邮箱：wangjh_yjs@dxzq.net.cn	执业证书编号：S1480519050004
研究助理	陈晓博 电话：010-66555574 邮箱：chenxb_yjs@dxzq.net.cn	执业证书编号：S1480119070046

投资摘要：

从合规和风险管理向数字化转型赋能转型，我国信息安全市场潜力仍巨大

全球企业都在将“数字化转型”作为重要的策略，“数字化转型”发展的加速，也给企业带来了新的安全风险。企业开始关注数字业务安全环境，从“预防”思维转变为更注重快速检测和应对能力的思维模式。全球 IT 支出的增长速度逐渐放缓，但是信息安全支出占 IT 支出的比重不断上升。根据 Gartner 的统计数据，全球信息安全支出占整个 IT 支出的比例越来越高，2018 年达到 3.05%。中国 2018 年的 IT 支出约 2.79 万亿元人民币，按全球 2018 年平均信息安全支出占比计算，我国信息安全市场潜在市场空间在千亿左右。

海外上云成主流，带动云安全服务市场快速发展

在全球市场中，信息安全市场以提供订阅化服务为主，2018 年，安全服务市场份额最大，占整个信息安全市场的 64.4%，而中国这一比例只有 15.6%。海外云计算市场发展较早，云服务渗透率远高于国内，安全订阅服务已经成为主流。根据国务院发展研究中心发布的《中国云计算产业发展白皮书》，2018 年，美国企业上云率已经达到 85%以上，欧盟企业上云率也在 70%左右，而中国各行业企业上云率只有 40%左右。2018 年全球云安全服务市场规模达到 60.2 亿美元，相比 2017 年增长 22.6%，增速接近网络安全整体市场的三倍。中国云安全市场目前仍处于起步阶段，云安全市场规模随云计算市场增长而快速崛起。根据赛迪数据，预计 2021 年中国云安全市场规模将达到 115.7 亿元，2019-2021 年年均增长率为 45.2%，行业正快速增长。

云安全市场格局：云服务商占主导，国内网安厂商发展机遇在私有云领域

根据 Forrester 数据，国外公有云原生平台安全占到 70%左右的营收，第三方安全厂商划分剩余市场份额。

国内云安全市场中，第三安全厂商的机会更多在私有云领域安全防护。一方面，公有云领域安全市场规模较小，根据 Gartner 数据，2020 年我国公有云服务安全市场预计可达 2.67 亿美元，占整体云安全市场的比重不到四分之一，而且公有云安全市场基本被云平台服务商占据，第三方安全厂家获利空间有限。另一方面，国内私有云建设仍是主流。根据中国信通院统计，2018 年中国云计算整体规模为 962.8 亿元，其中私有云市场规模 525 亿元，占比达 55%，仍高于公有云市场规模。政府和这些大型企业出于数据安全的担忧，首选的上云方式还是私有云或混合云，私有云和混合云领域的安全防护市场是第三方安全厂商在云安全领域的重要发展机会。

从海外网安龙头发展看国内安全厂商发展之路：私有云安全和安全运营是发展重点

CrowdStrike 作为一家云原生安全公司，从一开始就采取平台+模块的方式以 SaaS 订阅模式向客户提供服务，符合公有云环境下的用户习惯，实现了用户规模和营收的快速增长，也获得了较高的估值水平；Palo Alto 的特点在于产品齐全，能为各种用户提供全面的安全防护，公司跟随公有云的快速发展，推出安全订阅产品，实现公有云安全的突破，云安全作为公司安全业务之一起到协同带动作用，发展也相对稳定。

与全球信息安全市场相比，中国信息安全行业正处于快速成长期。传统的信息安全产品难以满足日益变化的复杂的网络空间，中国的信息安全行业必将向国际看齐，由硬件为主转换为服务为主。国内公有云安全市场目前尚小且主要被云服务提供商占据，国内安全产商的机遇在私有云和混合云领域。国内主要的安全厂商都开始全面布局云安全，并将私有云、行业云安全解决方案和安全运营作为发展重点。

推荐公司：云安全解决方案全面，前瞻布局城市安全运营的**启明星辰；**云计算与信息安全业务协同发展的**深信服；**专注新兴安全领域，“平台+服务”快速成长的**安恒信息。**建议关注：山石网科、三六零、绿盟科技等。

风险提示：疫情影响下游客户信息安全投入不及预期；政策实施不及预期；市场竞争加剧风险。

目 录

插图目录

表格目录

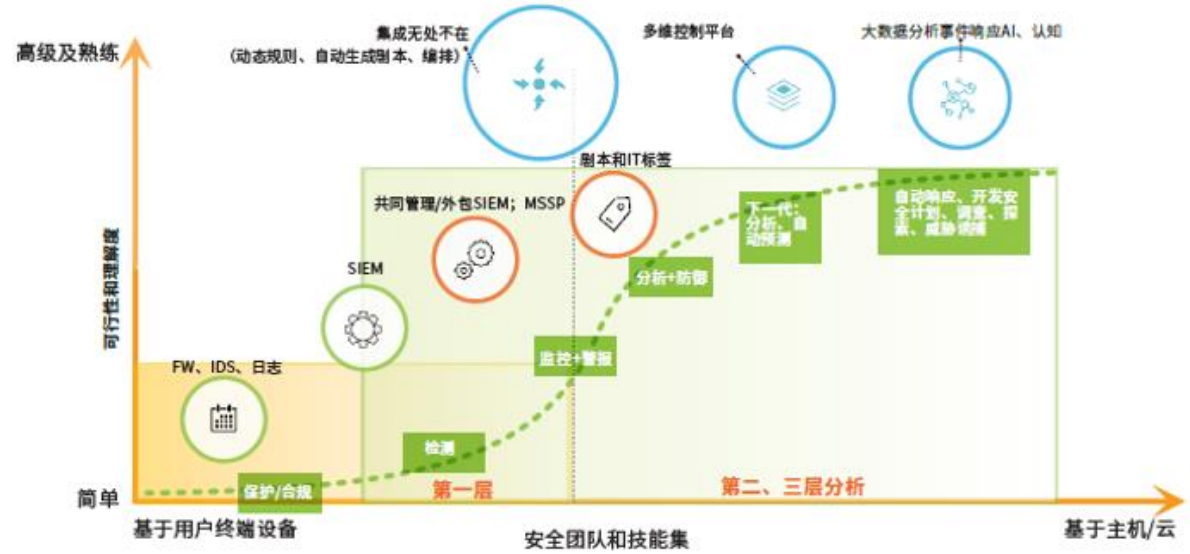
1. 信息安全：从合规和风险管理向数字化转型赋能转型

1.1 信息安全服务重要性凸显，为企业数字化转型保驾护航

如今全球企业都在将“数字化转型”作为重要的策略，企业也越来越依赖于将数据转变为有用的信息。但“数字化转型”发展的加速，也给企业带来了新的安全风险。随着安全威胁越来越隐蔽而难以发现，利用传统的被动防御工具已经越来越不能满足客户更高的安全需求。完全依赖厂商的被动式安全策略已经过时。企业必须开始关注数字业务安全环境，**从“预防”思维转变为更注重快速检测和应对能力的思维模式**。

从 20 世纪末简单的防火墙、入侵检测产品的部署到当今结构化的信息安全产品部署，随着安全防护要求的不断升级，信息安全技术也在持续演进和变革。下一代安全产品将广泛采用大数据分析、事件响应、AI、认知相关的技术。而信息安全防御体系也将向自动响应、开发安全计划、调查、追查、威胁诱捕等方向侧重，保障企业数字化转型的顺利进行。

图1：信息安全技术革新发展新方向



资料来源：IDC，东兴证券研究所

从网络安全层面，随着网络攻击行为日趋复杂，防火墙、IDS 等传统网络安全设备并不能完全阻挡恶意的网络攻击。构建全面的安全防护体系和制定完善的安全管理策略显得尤为重要，**风险评估、安全管理咨询、安全应急响应、安全托管服务的作用越来越受到用户重视。**

1.2 信息安全投入占 IT 总投入比重不断上升

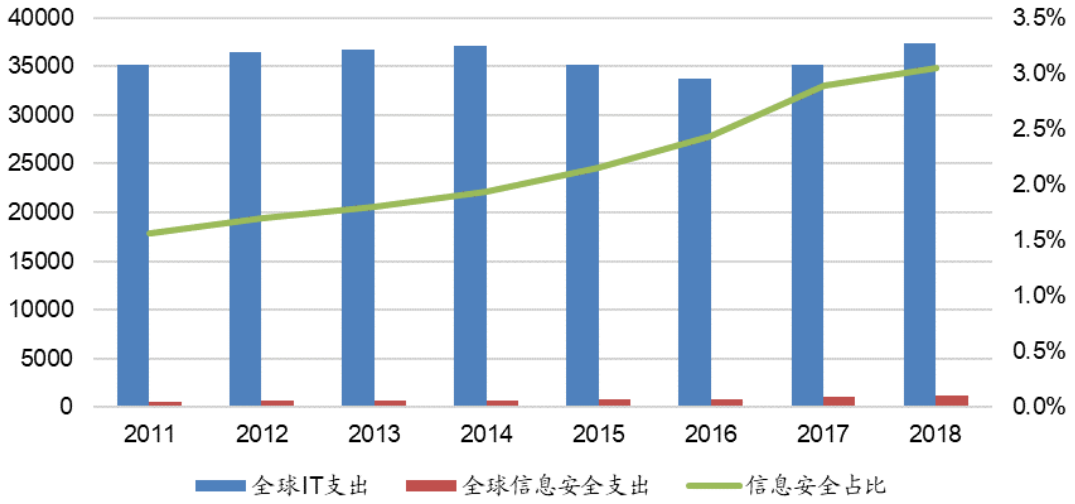
全球 IT 支出的增长速度逐渐放缓，但是信息安全支出占 IT 支出的比重不断上升。根据 Gartner 对 2011-2018 年全球 IT 支出及全球信息安全支出的统计数据来看，信息安全支出占整个 IT 支出的比例越来越高，2018 年达到 3.05%。

造成这一现象的主要原因有两点：一方面，企业的数字化经济转型中，IT 体系从原有的基础支撑，上升到业务驱动力，需要配套的信息安全可以满足业务灵活化、多样化及高用户体验等要求；另一方面，现实存在的

网络安全威胁日益复杂，而随着生产生活对于信息技术依赖提升，网络安全事件带来的社会影响和经济损失都日趋显著，信息安全监管随之加强，对企业的的信息安全管理及信息安全技术提出了更高更复杂的要求。

Gartner 数据显示,中国 2018 年的 IT 支出约 2.79 万亿元人民币,按全球 2018 年平均信息安全支出占比计算,我国信息安全市场潜在市场空间在千亿左右。

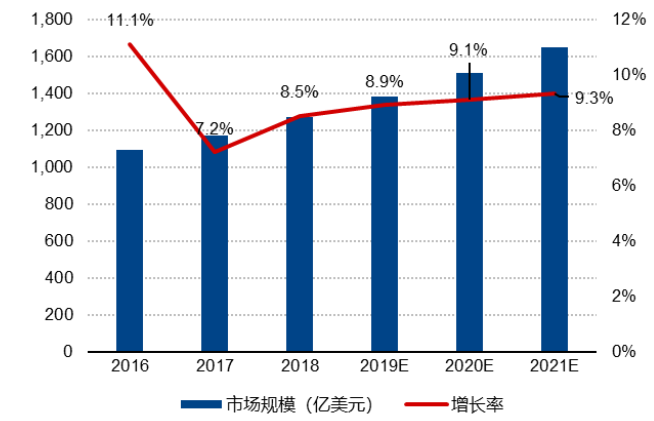
图2：全球 IT 支出及全球信息安全支出（亿美元）



资料来源：Gartner，东兴证券研究所

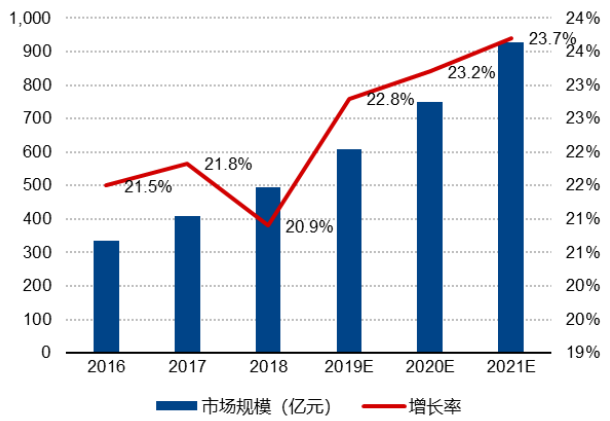
对比来看，我国信息安全产业还处于快速发展期，发展潜力巨大。根据赛迪顾问《2019 中国网络安全发展白皮书》，2018 年我国信息安全市场整体规模达到 495.2 亿元，较 2017 年增长 20.9%，远超全球安全市场整体增长率。以此数据计算 2018 年我国信息安全支出占 IT 总支出比重为 1.8%,和全球 2013 年平均水平相当。仍有较大提升空间。网络信息安全作为数字经济发展的必要保障，随着我国数字经济的发展，信息安全投入将持续增加。

图3：全球信息安全市场规模



资料来源：赛迪，东兴证券研究所

图4：我国信息安全市场规模



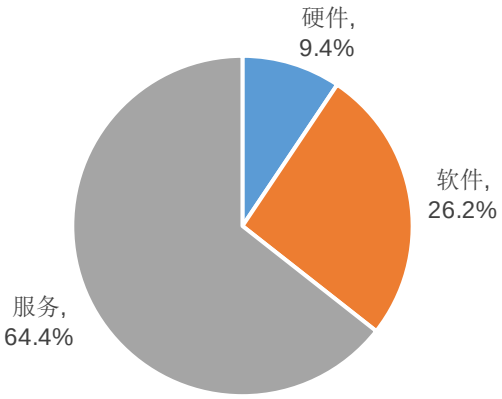
资料来源：赛迪，东兴证券研究所

2. 云安全需求不断提升

2.1 海外上云成主流，带动安全服务市场快速发展

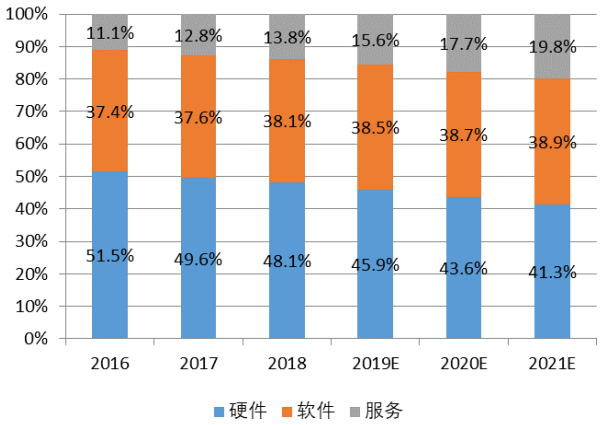
在全球市场中，网络安全市场以提供订阅化服务为主，2018 年，以安全服务市场份额最大，占市场的 64.4%；软件市场规模为 330.1 亿美元，占整体市场的 26.2%。而国内信息安全行业仍以安全硬件为主，与全球以安全服务为主的特点有着明显的差异。

图5：2018 年全球信息安全市场结构



资料来源：赛迪，东兴证券研究所

图6：我国信息安全市场结构



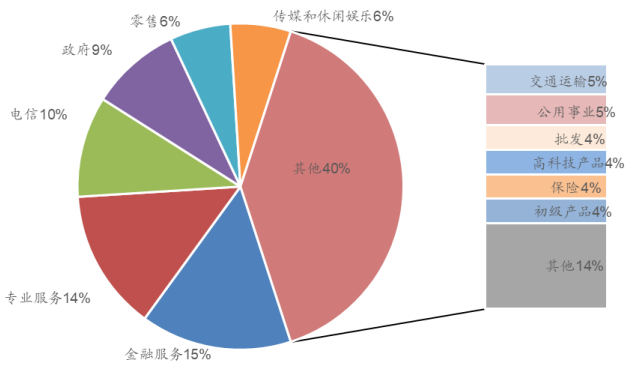
资料来源：赛迪，东兴证券研究所

究其原因，我们认为上述差异主要由两个因素导致：

- **一是在中国信息安全支出更多为合规驱动，主动防御意识弱，在预算体制下，安全产品更容易核算；**

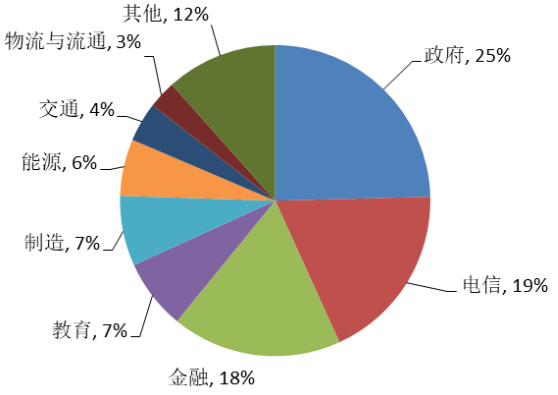
多年以来合规需求是驱动我国信息安全投入的主要因素。从下游需求来看，政府、电信和金融等涉及国家安全和国民经济命脉的行业是信息安全产品的主要需求对象，总占比超过 60%。在这些行业，对于信息安全都有相应的政策要求，企业受到政府监管要求而进行信息安全产品采购，所以满足合规需求成为我国信息安全市场增长的主要驱动力。

图7：美国云安全市场行业应用结构



资料来源：Forrester，东兴证券研究所

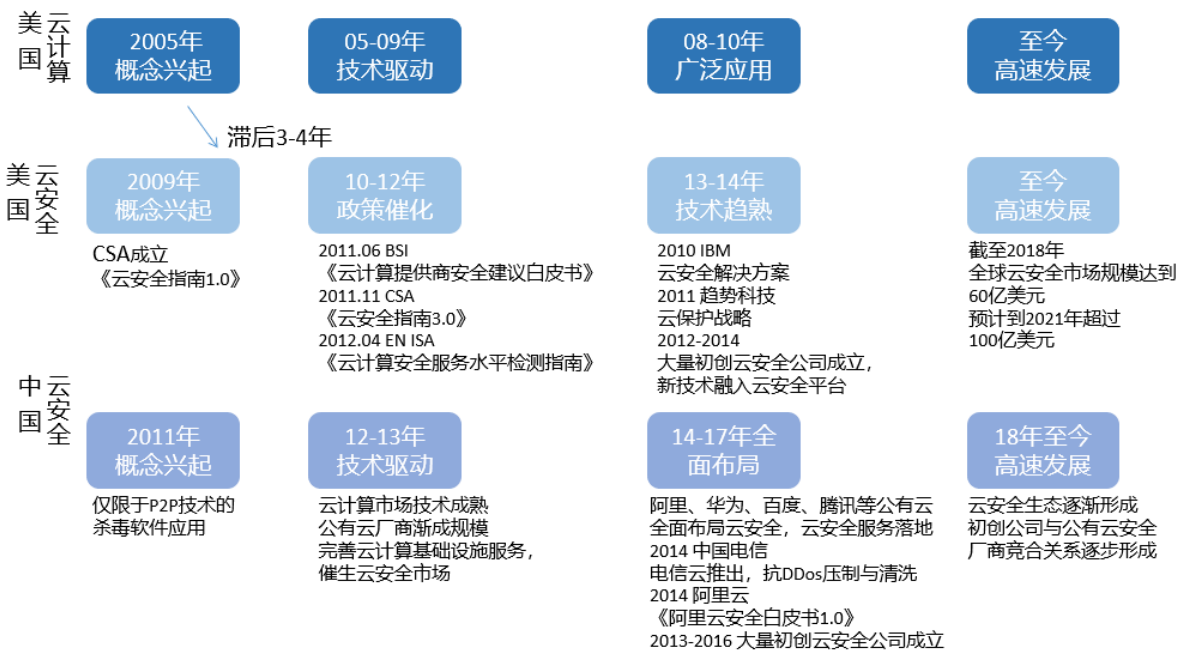
图8：中国信息安全市场行业应用结构



资料来源：赛迪，东兴证券研究所

➢ **二是海外云计算市场发展较早，云服务渗透率远高于国内，安全订阅服务已经成为主流，**根据国务院发展研究中心发布的《中国云计算产业发展白皮书》，2018 年，美国企业上云率已经达到 85%以上，欧盟企业上云率也在 70%左右，而中国各行业企业上云率只有 40%左右。从国际成熟市场经验来看，云安全行业发展滞后于云计算约 3-4 年时间。美国云计算行业从 2005 年开始，随后受技术驱动，2009 年后进入快速发展期。伴随着云计算行业发展，云安全服务行业经历了政策催化与技术驱动期，新技术与相应的初创公司不断涌现。中国云安全服务业的发展略晚于美国市场，2014 年阿里云等公有云厂商正式上线云安全服务，行业逐渐进入快速发展阶段。

图9：美国、中国云计算与云安全发展历程简略图



资料来源：Gartner，赛迪，东兴证券研究所

2.2 云安全伴随云计算快速崛起

2.2.1 云时代安全服务需求上升

云安全包含云计算安全与安全云服务两个方面。通俗地讲，云计算安全是保护云计算本身的安全，而安全云服务则是将安全作为云计算的一种服务。

表1：云安全具体含义

名称	含义
云计算安全	云计算自身的安全保护，包括云计算应用系统安全、云计算应用服务安全、云计算用户信息安全等。
安全云服务	以 SaaS 模式提供和交付安全，将云计算技术应用于网络安全，通过云化网络安全设施资源及业务能力，形成安全能力资源池，通过互联网为客户提供安全服务。

资料来源：公开资料整理，东兴证券研究所

自从 2006 年亚马逊 AWS 推出 EC2 之后，云计算的破坏性力量改变了整个科技行业。随后，国外的谷歌 GCP、微软 Azure 和国内的阿里云，进一步带动了整个云市场的发展。IaaS、PaaS、SaaS 的云计算分层结构被大家所熟知，公有云、私有云、混合云在每个单位云的建设中被反复提及。

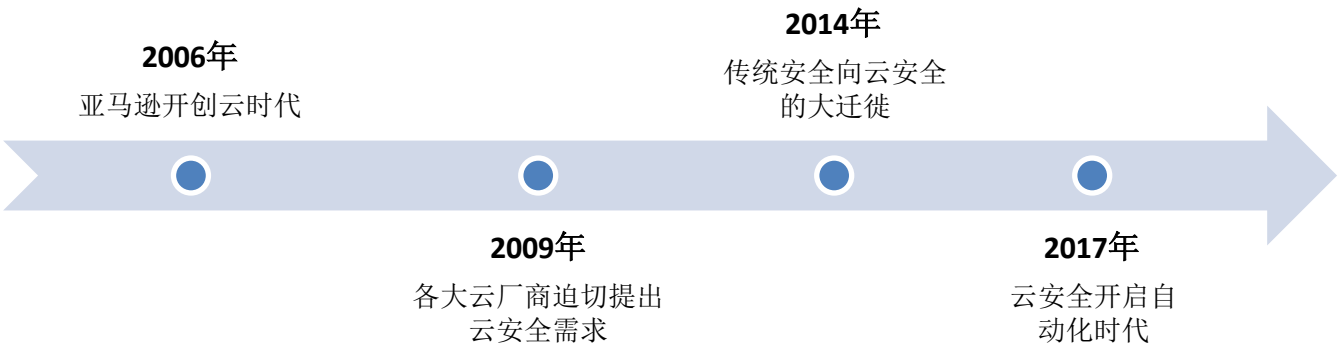
2009 年开始，苹果，微软，亚马逊，奥多比（Adobe），威睿（VMware）等公司开始在云中提供服务和应用程序，还为访问这些应用程序的用户提供云存储服务。通常由于应用程序本身在云上运行，因此无需在用户的终端系统上安装或存储任何内容。

这一转变给互联网管理员和安全专家们带来了空前挑战。随着应用程序，数据，用户信息和公司敏感数据越来越多地存储在云中，而不是公司网络中，经典的辐射式中心安全模型在云优先选择的压力下开始崩溃。随后，安全软件和硬件供应商开始了同样的转变。

到了 2014 年，云安全服务的提供商开始提供域名系统（DNS）保护，电子邮件安全，内容过滤和其他各种工具，从而减少了对设备硬件的依赖性，降低了回程成本，帮助使用多个传统信息安全厂商的公司进行整合并把他们迁移到云端。

到了 2017 年，Zscaler 和 OpenDNS 之类的公司发布了功能全面的基于云的下一代防火墙（NGFW）服务，大大降低了成本与非云设备硬件的功能相媲美甚至超越了非云设备硬件的功能。公司不仅可以离开设备传送带，而且还可能淘汰所有安全设备。拥有多个办公室的公司正在回程传输到中心办公室的流量，通常每年仅在电信成本方面就节省了成千上万的费用，因为他们不再需要回头穿过中心办公室。

图10：国外云安全发展简要历程



资料来源：公开资料整理，东兴证券研究所

云计算的进步带动无服务器计算发展，也引发了新的网络信息安全问题。攻击者更容易借无服务器计算隐藏活动踪迹制造网络威胁。这些都成为云计算发展过程中带来的网络信息安全威胁，同时也为云安全产品与服务的研发与部署提供了广阔的应用场景。公有云的多租户共享场景将导致可信边界的弱化，威胁的增加，因此构建基于云的纵深防护体系成为应对公有云安全威胁的重要手段。私有云、行业云领域，众多厂商积极在云安全资源池、云工作负载保护平台等重点领域加速布局。

云是一个复杂的系统，云安全的需求散布在云的各个层次、各个环节。我们可以从角色划分、系统架构、服务层次和部署方式四个角度来呈现云安全需求的面貌。

表2：云安全模型中的需求分布

	层级细分	具体需求
角色划分	云厂商	边界保护，安全功能隔离，资源优先级与调度，应用分隔
	云租户	账户管理，开发者配置管理，用户身份认证，密钥分发与管理，缺陷修复
	第三方审计人	安全评估，安全证明，安全鉴定
系统架构	物理资源层	身份认证与管理，基础设施安全，数据隐私保护，数据传输安全，审计与合规性，数据完整性，网络攻击防范
	资源抽象和控制层	虚拟机安全，基础设施安全，租户隔离，身份与访问管理，法律与合规
	服务层	静态数据保护，物理安全，网络和服务器安全
服务层次	SaaS 层	登陆安全，访问控制，数据与隐私保护
	PaaS 层	安全设计，安全编程，安全测试，安全发布
	IaaS 层	存储安全，数据完整性，冗余备份，审计计费安全
部署方式	私有云	为单一用户提供云服务，外包私有云的访问控制，边界保护
	公有云	为多个云租户提供云服务，云租户共享云资源，工作环境隔离
	社区云	
	混合云	

资料来源：公开资料整理，东兴证券研究所

近年来，云安全市场表现出了两大趋势特征：大规模 DDoS 攻击事件的升级和联网设备数量激增导致安全威胁无孔不入。一是大流量 DDoS 攻击成为新常态。2019 年 2 月，GitHub 遭遇了带宽 1.35T 的 DDoS 攻击。同年 11 月，网宿科技宣布其云安全平台防御了一起攻击流量为 1.02T 的 DDoS 攻击事件。二是联网设备数量激增及入口碎片化，让安全威胁变得无处不在。跟据 Gartner 的数据，联网设备数量到 2020 年底将由 2017 年的 84 亿部增至 266 亿部，涵盖了家居设备、安防、智能汽车、医疗设备等各个场景，这必然催生出更多样化、更复杂的云安全需求。这意味着安全态势发生了转变，仅靠传统的集中式、本地化的防护远远不够了，如防火墙、杀毒、WAF、漏洞评估等以防御为主的安全软硬件方案，已经难以适应物联网、云计算架构下的安全需求了。

表3：云安全的需求变化

	2013 年	2015 年	2017 年	2019 年
DDoS 攻击事件升级	300G 级带宽	600G 级带宽	345G 级带宽	1.3T 级带宽
联网设备数量激增	75 亿部	130 亿部	180 亿部	230 亿部

资料来源：公开资料整理，东兴证券研究所

表4：云安全和传统信息安全的对比

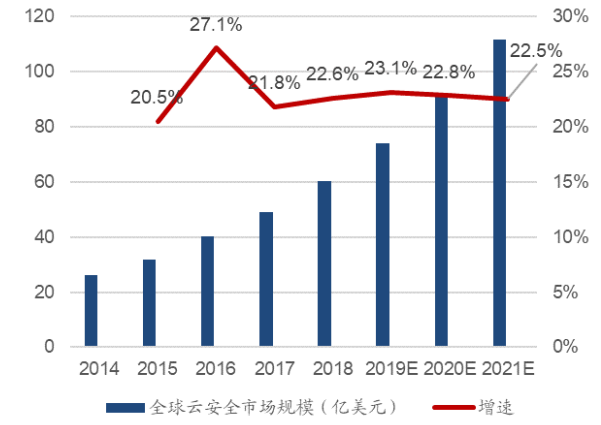
	传统信息安全	云安全
安全隐患	网络层和主机层的安全漏洞和威胁	传统安全隐患以及云计算虚拟化、数据及服务外包和共享技术带来的安全漏洞
保护重点	计算、网络和存储资源	传统保护对象以及虚拟化安全
安全技术	加密、安全监测等	并行处理，网格计算
保护规模	单机数据	云数据资源

资料来源：公开资料整理，东兴证券研究所

根据 Gartner 统计，2018 年全球云安全服务市场规模达到 60.2 亿美元，相比 2017 年增长 22.6%，增速接近网络安全市场的三倍。云技术作为未来的主流技术趋势，以云技术为依托的云安全服务是未来发展方向，未来云安全市场将持续扩大，云抗 DDoS、云 WAF、云身份管理、云基础架构安全、云主机安全等云安全服务细分市场将迎来高速发展时期，赛迪预计，到 2021 年全球云安全服务市场规模将达到 111.5 亿美元，2019-2021 年年均增长率为 22.8%。

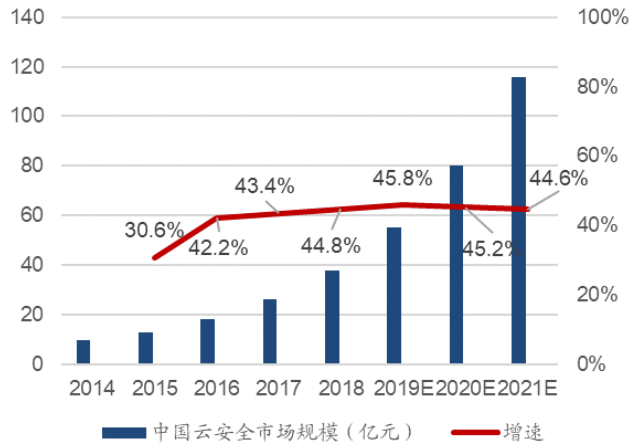
中国云安全市场目前仍处于起步阶段，整体的市场规模随着云计算市场规模的增长而快速崛起。根据赛迪顾问数据，中国云安全整体的市场规模会随云计算市场增长而快速崛起。预计到 2021 年中国云安全服务市场规模将达到 115.7 亿元，2019-2021 年年均增长率为 45.2%，行业正快速增长。

图11：全球云安全市场规模



资料来源：Gartner，赛迪，东兴证券研究所

图12：中国云安全市场规模



资料来源：赛迪，东兴证券研究所

3. 云安全市场格局：云服务商占主导，国内网安厂商发展机遇在私有云领域

云安全产品可以分为两类，一类是云计算提供方直接提供的安全产品，另一类是第三方安全厂商提供的安全产品。就公有云来说，基础架构安全一般由云厂商负责，而工作负载安全则由云租户负责。人们常常认为私有云更安全，是因为工作负载通常是在用户自己的防火墙后面运行，因此部署的私有云资源越多，需要购买或租借的硬件就越多，运维成本也就越高。在混合云中，云租户可以根据具体情况，自行选择是要承担横向扩展所产生的运维开支，还是要承担纵向扩展所产生的资本开支。

总的来说，云厂商的安全需求可以概括为平台级的安全防护、等保合规和安全运营。云租户的安全需求则是自服务的安全防护，创建防火墙，边界防御等。**国内外的云服务供应商，如阿里云、腾讯云和 AWS 等都提出了责任共担模型来明确与租户之间的安全责任划分。**

以腾讯云为例，腾讯云基于信息资产和产品功能建立了如下的信息安全责任共担模型，其中定义浅蓝色部分由腾讯云负责，浅灰色部分为客户负责，浅绿部分则表示腾讯云和客户将共同承担相应的责任。

IaaS 架构模型中：腾讯云为客户提供的是基础云产品，类型主要包括云主机、云存储、负载均衡、物理服务器、CDN 等。

腾讯云对虚拟化控制层、数据库管理系统、磁盘阵列网络等云产品底层系统提供包括漏洞发现、补丁修复、升级更新、审计监控等安全管理措施；此外，腾讯云提供基础的外部 DDoS 防护能力，以保护处于云计算平台网络中的各类资源不受来自互联网的拒绝服务攻击影响；

客户需对已购买的云主机的操作系统、数据库实例文件、云主机间的网络通信、以及由内向外的网络通信等加以安全控制。客户有责任维护并管理已购买的云产品和内部数据，类似如因客户管理不当造成的云主机主动或被动向外发起恶意攻击（如大流量 DDoS 攻击、网络嗅探、病毒木马攻击等）的情况则不在腾讯云的责任范围。

PaaS 架构模型中：腾讯云为客户提供的是平台类云产品，类型主要包括云数据库、云缓存、音视频云通信等。应用安全和访问控制管理由客户与腾讯云共同承担。

SaaS 架构模型中：腾讯云为客户提供的是应用类云产品，类型主要包括云通信、云搜、优图人脸识别等。访问控制管理和终端安全由客户与腾讯云共同承担。

图13：腾讯云安全责任共担模型

资料来源：腾讯云，东兴证券研究所

基于阿里云的客户应用，其安全责任由双方共同承担：阿里云要保障云平台自身安全并提供安全产品和能力给云上客户；客户负责基于阿里云服务构建的应用系统的安全。

图14：阿里云安全责任共担模型

资料来源：《阿里云安全白皮书4.0》，东兴证券研究所

云服务提供商根据责任共担模型划分安全责任，提供履行自身责任的安全产品，保证基础设施安全并提供标准化安全服务。云服务提供商提供安全产品的目的不是全面保障客户的安全，而是让客户使用云的时候能够安全，简单来说就是如何安全的使用云计算。以 AWS 为例，其平台提供的原生的安全产品包括五个方面：身份访问控制类、检测式控制类、基础设施保护类、数据保护类及合规类型。

拿行业排名前两位的亚马逊 AWS 和微软 Azure 来说，这两家云厂商在云安全领域所能提供的产品和服务如下表所示：

表5：亚马逊 AWS 与微软 Azure 功能对比

功能	亚马逊 AWS 服务	微软 Azure 服务	功能说明
身份验证与授权	身份和访问管理（IAM）	活动目录（AAD） 基于角色的访问控制（RBAC）	允许用户安全地控制对服务和资源的访问，并提供数据安全和保护。 创建并管理用户和组，并使用权限允许和拒绝访问资源。 RBAC 可帮助管理谁有权访问 Azure 资源、可以对这些资源执行哪些操作以及有权访问哪些区域。
	组织（Organizations）	订阅管理 + RBAC	处理多个帐户的安全策略和角色管理。
	多重身份验证（MFA）	多重身份验证	保护对数据和应用程序的访问，同时满足用户对简单登录过程的需求。
	目录服务	AAD 域服务	提供与 Windows Server Active Directory 完全兼容的托管域服务，例如域加入、组策略、LDAP 和 Kerberos/NTLM 身份验证。
加密	采用 AMS 密钥管理服务（KMS）的服务器端加密	Azure 存储服务加密	帮助保护数据，使组织能够信守在安全性与符合性方面所做的承诺。
	云硬件安全模块(CloudeHSM)	Key Vault	通过提供一种管理、创建和控制存储在 HSM 中加密密钥的方法，提供安全解决方案并与其他服务配合使用。
安全性	Amazon Inspector	Asure 安全中心	自动安全评估服务，可以提高应用程序的安全性和适配性。系统会自动评估应用程序的漏洞或与最佳算法的偏差。
	证书管理器	门户中提供的应用服务证书	允许客户在云中无缝创建、管理和使用证书的服务。
	GuardDuty	高级威胁防护（ATP）	在本地和云中检测和调查高级攻击。
	项目（Artifact）	服务信任门户	允许通过云服务访问审核报告、符合性指南和信任文档。
	盾（Shield）	DDos 保护服务	保护云服务免受分布式拒绝服务(DDoS) 攻击。

资料来源：公开资料整理，东兴证券研究所

从收入层面来看，根据 Forrester 数据，国外公有云原生平台安全占到 70%左右的营收，第三方安全厂商划分剩余市场份额。AWS 对于云安全责任共担模型的理解以及安全生态的重视，形成了目前的一系列合作伙伴产品在 market place 上售卖。AWS 友好的安全类型的 API，让很多云安全厂商可以很好的利用这些 API 来开发基于 AWS 的安全产品，这也引导了 Azure 和 GCP 的云安全建设思路，国外的很多云安全公司都在利用这些平台的 API 来开发自己的安全产品，在基础数据收集以及展示方面能极大的减少开发的复杂度。

图15：AWS 平台安全产品

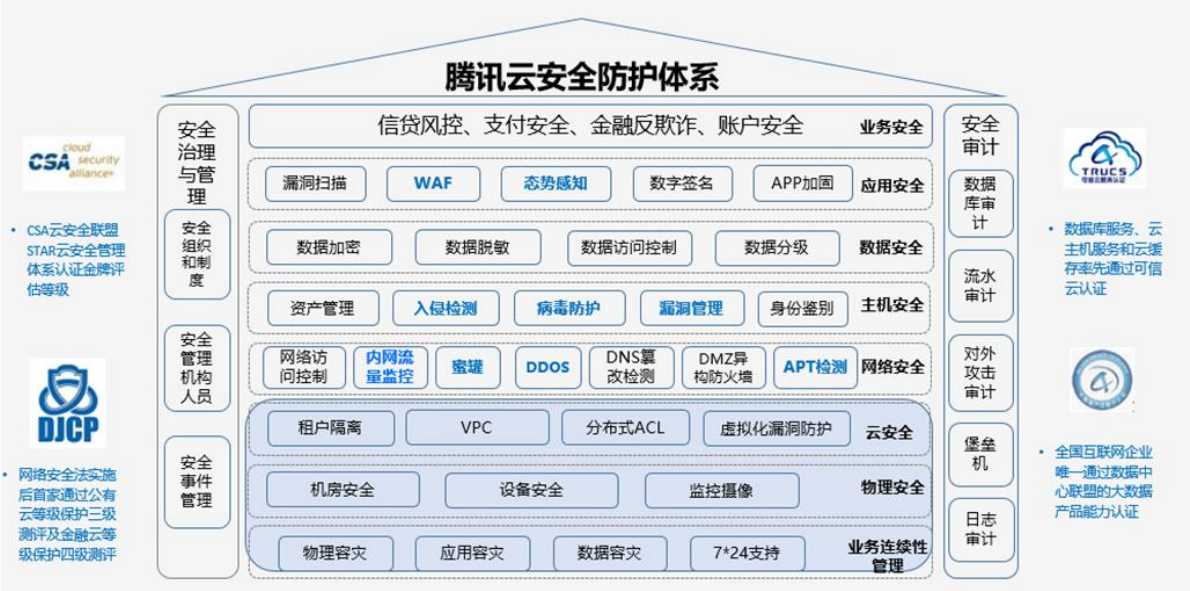
类别	使用案例	AWS 服务
Identity & Access Management	安全地管理对服务和资源的访问	AWS Identity & Access Management (IAM)
	云单点登录 (SSO) 服务	AWS Single Sign-On
	应用程序身份管理	Amazon Cognito
	托管的 Microsoft Active Directory	AWS Directory Service
	用于分享 AWS 资源的简单而安全的服务	AWS Resource Access Manager
检测式控制	一体化安全性与合规性中心	AWS Security Hub
	托管的威胁检测服务	Amazon GuardDuty
	分析应用程序安全性	Amazon Inspector
	调查潜在的安全问题	Amazon Detective
基础设施保护	DDoS 保护	AWS Shield
	过滤恶意 Web 流量	AWS Web 应用程序防火墙 (WAF)
	集中管理防火墙规则	AWS Firewall Manager
数据保护	大规模发现和保护您的敏感数据	Amazon Macie
	关键存储和管理	AWS Key Management Service (KMS)
	有助于实现监管合规性的基于硬件的密钥存储	AWS CloudHSM
	预置、管理和部署公有和私有 SSL/TLS 证书	AWS Certificate Manager
	轮换、管理和检索密钥	AWS Secrets Manager
合规性	免费的自助门户，允许按需访问 AWS 合规性报告	AWS Artifact

资料来源：AWS 官网，东兴证券研究所

而在国内，公有云领域安全市场基本被云平台服务商占据，第三安全厂商的机会更多在私有云领域安全防护，主要原因有两点：

- **一是国内阿里云、腾讯云、华为云等云平台服务提供商倾向于自己建立云安全服务体系，**提供标准化、基础性产品，包括了从 DDoS 高防、主机安全、Web 应用防火墙、网站威胁扫描系统、加密服务、态势感知到安全专家服务等 20 余项。
- **二是公有云用户对于安全服务付费意愿低。**国内公有云用户主要是 B 端中小型客户，对属于成本项的信息安全支出付费意愿较低，同时，云安全责任共担模型没有地传导到消费者端，用户更多采用平台自带的免费安全防护产品。另外，云平台服务提供商自己也提供付费高级安全防护服务，用户即使有较高防护需求也更倾向于云服务商提供的高级防护需求。

图16：腾讯云安全产品

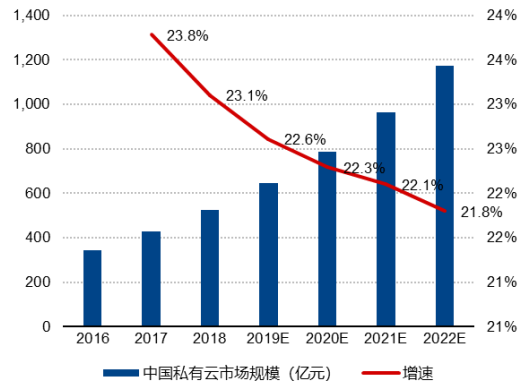


资料来源：腾讯开放平台，东兴证券研究所

出现上述差异情况的原因跟云计算发展的阶段和模式有关，国外已经成为云计算双头垄断 AWS 和 Azure，且公有云占主导地位，而国内私有云和行业云的占比更高。根据中国信通院统计，2018 年中国云计算整体规模为 962.8 亿元，其中私有云市场规模 525 亿元，占比达 55%，仍高于公有云市场规模。根据 Gartner 数据，2020 年我国公有云服务安全市场预计可达 2.67 亿美元，占整体云安全市场的比重不到四分之一。

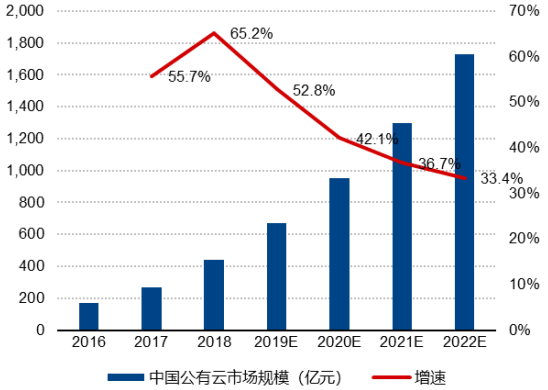
本身技术和投入有关，私有云和混合云采用安全方案的时候，更多的是采用第三方的安全供应商、云平台本身提供的安全产品以及外采服务三种形式混搭的情况，同时第三方安全产品的选择比例高于另外两者。未来，随着我国政府和企业业务创新，同时伴随着数字化、网络化、智能化转型需求的提升，预计政府和大型企业上云趋势将加速发展，到 2023 年中国政府和大型企业上云率将超过 60%。**而政府和这些大型企业出于数据安全的担忧，首选的上云方式还是私有云或混合云，所以私有云和混合云领域的安全防护市场是第三方安全厂商在云安全领域的重要发展机会。**

图17：中国私有云市场规模



资料来源：中国信通院，东兴证券研究所

图18：中国公有云市场规模



资料来源：中国信通院，东兴证券研究所

4. 从海外网安龙头发展看国内安全厂商发展之路

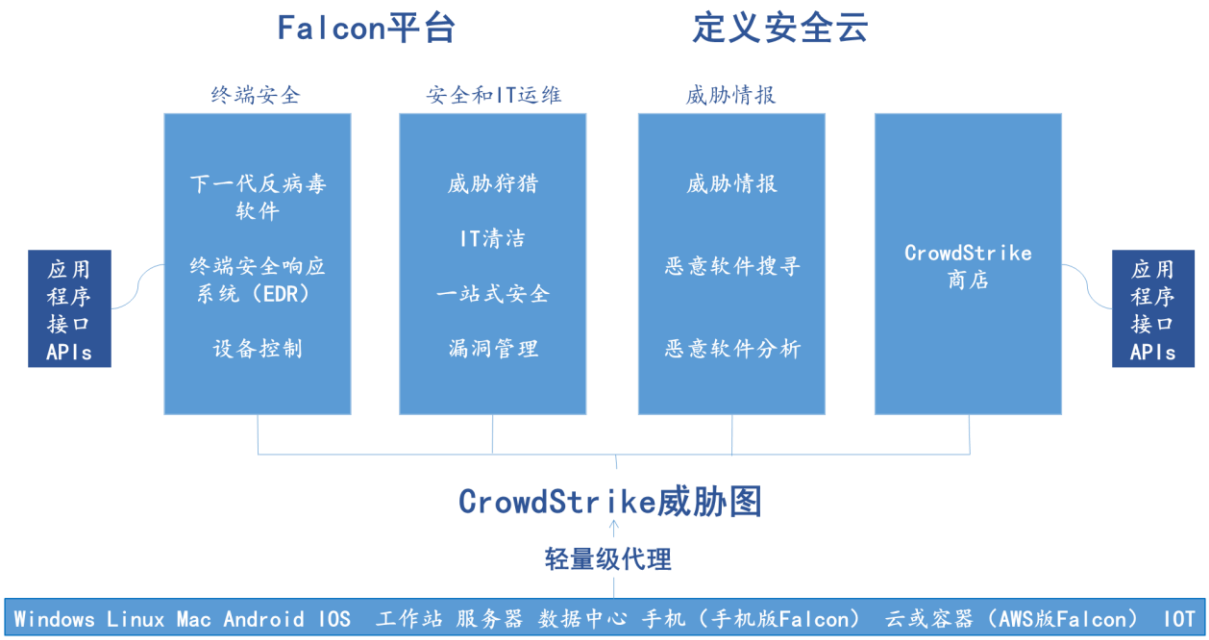
4.1 CrowdStrike：云安全龙头企业

4.1.1 主要产品：平台+模块化产品，SaaS 订阅

CrowdStrike 成立于 2011 年，公司总部位于美国加州，员工总数 2309 人（截止 2020.4.30），是一家网络安全软件开发商，致力于重塑云时代的安全性。公司于 2019 年 6 月 12 日在纳斯达克上市，公司 2020 财年（截止 2020.01.31）营业收入规模为 4.81 亿美元，截止 2020 年 6 月 23 日公司市值为 225 亿美元，是云安全领域龙头公司。

为了应对云时代的网络安全问题，公司构建了 CrowdStrike Falcon 平台来检测威胁并阻止漏洞，并借助 Falcon 平台构建了第一个多租户，云原生，开放，智能的安全解决方案。

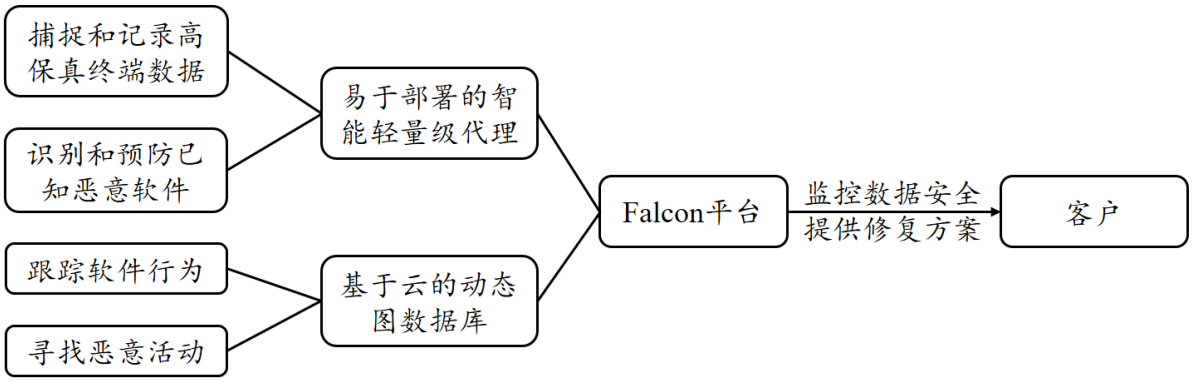
图19：CrowdStrike 公司 Falcon 平台



资料来源：公司公告，东兴证券研究所

Falcon 平台的核心技术包括易于部署的智能轻量级代理和基于云的动态图数据库。前者可以捕捉和记录高保真终端数据、识别和预防已知恶意软件；后者则跟踪软件行为、寻找恶意活动。Falcon 平台基于二者的技术支持，监控客户数据安全，并为其提供修复方案。

图20：CrowdStrike 公司 Falcon 平台工作模式示意图



资料来源：公司官网，东兴证券研究所

Falcon 平台通过基于 SaaS 订阅的模型集成了 11 个云模块，该模型跨越多个大型安全市场，包括终端安全，安全和 IT 运维（包括漏洞管理），以及威胁情报，即使在当今最复杂的攻击中也可以提供全面的安全保护，公司通过出售平台和云模块来获取订阅收入。根据公司 2020 财年全年财务报告，公司收入来源于订阅和专业服务两部分，其中订阅收入占总收入的 90%以上。

表6：CRWD 产品模块及特点描述

产品类型	产品模块	特点描述
终端安全 (Endpoint Security)	Falcon Prevent（下一代防病毒）；Falcon Insight（EDR）；Falcon Device Control（设备控制）	结合了机器学习和先进的行为技术，可抵御恶意软件和无恶意软件的攻击。 实现连续，全面的**可见性和端点活动分析**，并为管理员提供跨 USB 外围设备的可见性和精细控制。
安全和 IT 运营 (Security and IT Operations)	Falcon OverWatch（威胁狩猎）；Falcon Discover（IT 监察）；Falcon Complete（一站式解决方案）；Falcon Spotlight（漏洞管理）	实时识别客户终端中存在的漏洞，为企业的漏洞暴露提供即时，准确的实时可视化；由安全专家团队提供支持，提供**监控、管理、响应和修复**解决方案。
威胁情报(Threat Intelligence)	Falcon X（威胁情报）；Falcon Search Engine（恶意软件搜寻）；Falcon Sandbox（恶意软件分析）	提供自动协助，将威胁情报集成到终端保护中，对检测到的威胁自动分析，并将其及其变体的保护扩展到企业内部的其他安全解决方案中，进行恶意软件研究并安全清除可疑文件。

资料来源：公司公告，东兴证券研究所

4.1.2 业务模式：直销为主，模块化订阅

公司主要通过直接销售团队销售 Falcon 平台和云模块，该团队包括现场销售和内部销售专业人员，这些人员按客户的终端数量进行细分。通过细分销售团队，公司可以部署低接触销售模型，以有效地识别潜在客户。

公司也可以利用销售团队来确定对其他云模块的免费试用感兴趣的客户，采用**登陆再扩张（land and expand）战略，**即当客户部署 Falcon 平台时，他们可以从任意数量的云模块开始，并且公司可以在已经部署在终端上的同一代理实时激活其他云模块。这种架构还使公司能够直接从网站或 AWS Marketplace 开始免费提供

Falcon Prevent 模块的试用版，并且计划将来将此功能扩展到其他模块。一旦客户体验了 Falcon 平台的优势，他们通常会通过购买更多的终端或模块来扩展其使用范围。

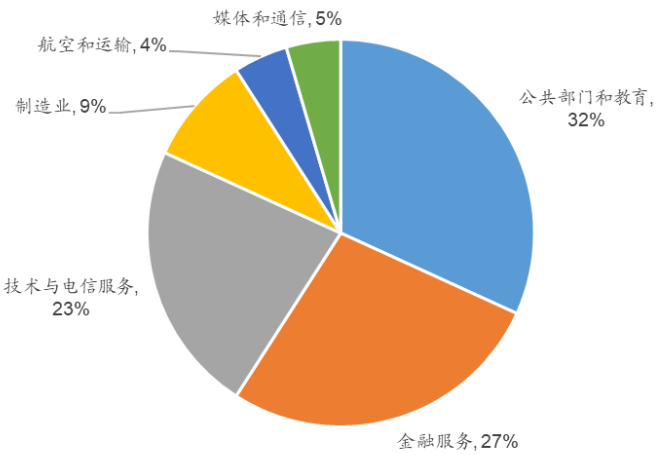
从 2017 年 12 月开始，公司开始采用试用付款模式，让潜在客户免费试用 Falcon Prevent 15 天。2018 年 5 月，公司宣布 Falcon Prevent 可从 AWS Marketplace 进行试用和购买。

公司最初是为大型企业提供的解决方案，但是 Falcon 平台的灵活性和可扩展性使公司能够无缝地为各种规模的客户提供解决方案，从拥有数十万个终端的客户到多达三个终端的客户。公司已将销售重点扩大到包括任何组织。

4.1.3 核心客户：大型组织为主，逐步拓展中小客户

截至 2020 年 4 月 30 日，公司在全球拥有 6,261 个订阅客户，其中包括《财富》100 强公司中的 49 家，全球前 100 名公司中的 40 家以及前 20 名中的 11 家主要银行，例如亚马逊、汇丰银行、凯悦酒店等。从历史上看，公司和渠道合作伙伴主要销售给大型组织，但近年来越来越关注于销售给小型组织和中型企业，尤其是通过“试用付款”模式。

图21：CRWD 部分客户行业分布



资料来源：公司官网，东兴证券研究所

4.1.4 订阅收入为主，仍处于快速增长期

CrowdStrike 的收入由两部分构成：订阅收入（Subscription revenues）和专业服务和其他收入（Professional servicesrevenues）。其中订阅收入就是 SaaS 产品的年费及在订阅期内对订阅服务的相关支持和更新的费用，专业服务收入包括包括事件响应和主动服务的收入，公司提供专业服务的安排主要基于时间和材料。

表7：CRWD 主要财务数据

单位：百万美金	Q3 2019	Q4 2019	Q1 2020	Q2 2020	Q3 2020	Q4 2020	Q1 2021
	10/31/2018	01/31/2019	04/30/2019	07/31/2019	10/31/2019	01/31/2020	04/30/2020
营收	**66.38**	**80.46**	**96.08**	**108.11**	**125.12**	**152.11**	**178.08**
YoY		108%	103%	94%	88%	89%	85%
订阅收入	**57.65**	**72.83**	**85.99**	**97.58**	**114.22**	**138.54**	**162.22**
YoY		124%	116%	98%	98%	90%	89%

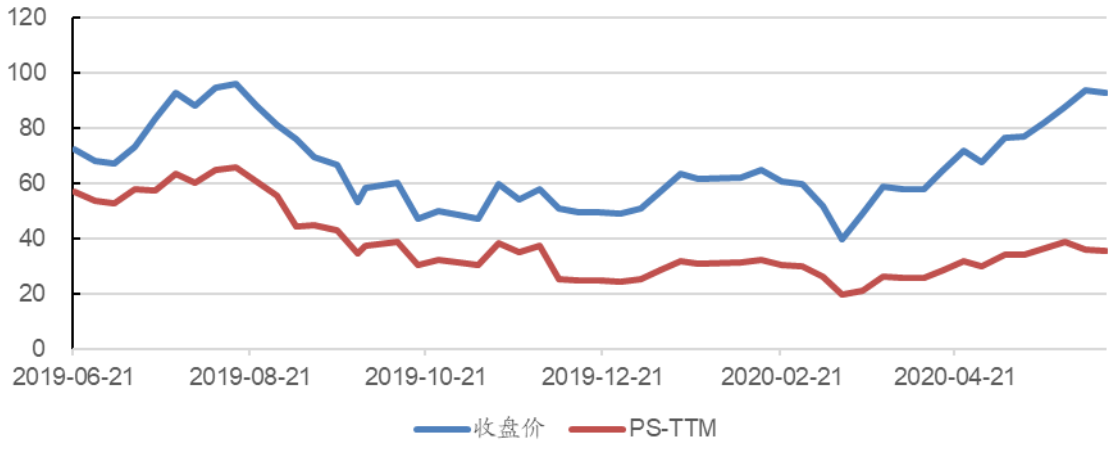
单位：百万美金	Q3 2019	Q4 2019	Q1 2020	Q2 2020	Q3 2020	Q4 2020	Q1 2021
	10/31/2018	01/31/2019	04/30/2019	07/31/2019	10/31/2019	01/31/2020	04/30/2020
专业服务收入	8.73	7.62	10.09	10.53	10.90	13.57	15.86
毛利率	**66%**	**66%**	**70%**	**71%**	**70%**	**71%**	**74%**
销售占比	**70%**	**61%**	**59%**	**60%**	**55%**	**50%**	**49%**
研发占比	**39%**	**27%**	**25%**	**29%**	**29%**	**25%**	**23%**
管理占比	**21%**	**17%**	**12%**	**28%**	**17%**	**17%**	**14%**
营业利润率	-63.41%	-38.58%	-26.83%	-48.30%	-30.79%	-20.47%	-12.68%
经营活动所得现金			**1.42**	**-6.21**	**38.64**	**66.11**	**98.58**
订阅客户(个)	**2,147**	**2,516**	**3,059**	**3,789**	**4,561**	**5,431**	**6,261**
YOY	155%	103%	105%	111%	112%	116%	105%
ARR	254	313	365	424	502	600	686
YOY	124%	121%	114%	104%	97%	92%	88%
客单价(万元)	118	124	119	112	110	111	110

资料来源：Bloomberg，公司公告，东兴证券研究所

受益于云安全市场的快速发展，公司收入快速增长，2021 财年 Q1，公司营收为 1.78 亿美元，同比增长 85%。其中订阅收入为 1.62 亿美元，收入占比为 91.1%。随着营业收入的增长，规模效应逐渐显现，公司的毛利率不断提升，期间费用率逐渐下降。

对 SaaS 公司估值基本采用市销率来估值，市销率高低主要取决于收入增速，公司上市后股价与市销率基本保持相同趋势。公司市销率随着营收增速的放缓有所下降但仍保持较高水平。当前市销率水平在 35 倍左右。

图22：CRWD 估值情况



资料来源：wind，东兴证券研究所

4.2 Palo Alto Networks：转型云安全，实现增长提速

4.2.1 主要产品：以防火墙为基础，产品+SaaS 订阅

Palo Alto Networks（PANW.O）创立于 2005 年，总部位于美国加利福尼亚州，员工总数 7,041 人（截止 2019.07.31），是一家网络及资讯安全软件提供商，公司自 2007 年以来开始提供防火墙产品。除企业防火墙物理和虚拟设备外，公司产品还包括 EDR 软件，威胁情报，SaaS 安全性，云遵从性和策略管理工具以及安全流程，自动化和响应（SOAR）等产品。

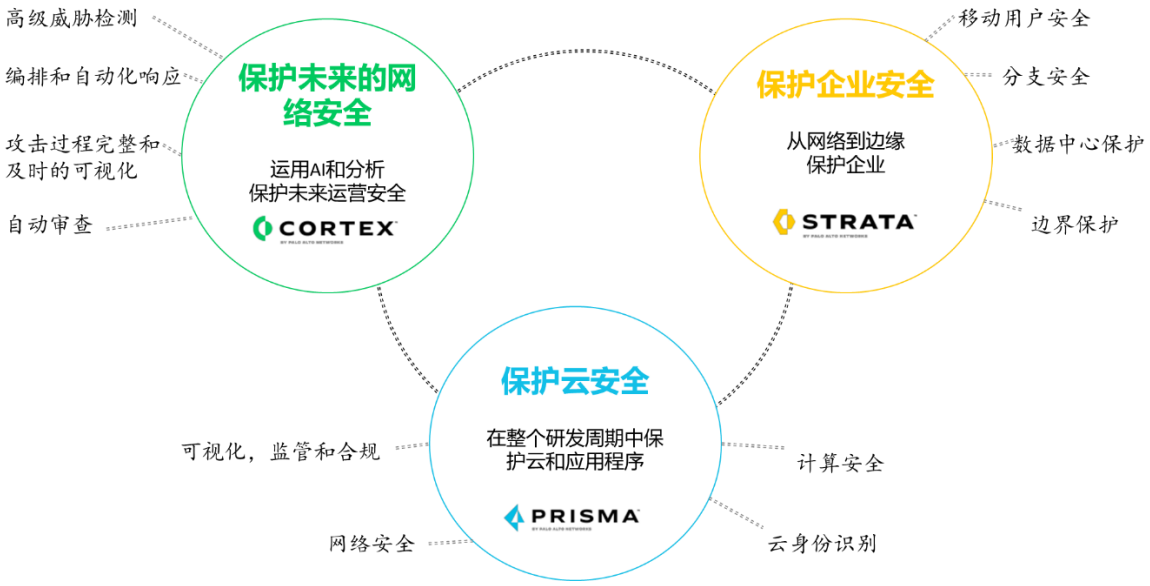
公司 2012 年 7 月在纽交所上市，公司 2019 财年（截止 2019.07.31）实现营收 29 亿美元，截止 2020 年 6 月 23 日公司市值为 221 亿美元。公司连续 8 次成为 Gartner 防火墙魔力象限领导者，是网络安全领域龙头公司。

图23：Gartner 防火墙魔力象限

资料来源：Gartner，东兴证券研究所

Palo Alto Networks 公司通过创新平台开创了下一代安全性，该平台从企业安全、云安全、下一代安全三个方面使企业，云服务提供商和政府等能够安全地启用在其网络，终端和云中运行的应用程序和数据，并防止数据泄露，让企业具备一流的检测、调查、自动化和响应能力，保护其系统的安全。

图24：Palo Alto 业务分布



资料来源：公司公告，东兴证券研究所

公司开展的业务包括产品，订阅服务、支持服务以及专业服务。

表8：公司安全产品和服务

业务分类		业务名称	特点描述
产品		防火墙设备和软件	可针对不同性能要求、吞吐量提供一致安全服务，可以以物理形式和虚拟形式出现。
		Panorama	用于控制网络以及公共或私有云环境中的的所有防火墙设备和软件。用于集中式策略管理，设备管理，软件许可和更新，集中式日志记录和报告以及日志存储。
		虚拟系统升级	虚拟系统容量的扩展提供，可为同一硬件设备上的租户提供多种不同的安全策略和管理访问权限，适用于大型企业和服务提供商终端客户。
订阅服务	企业安全	威胁防护	入侵检测和防御功能，可以阻止漏洞利用，病毒，间谍软件，缓冲区溢出，拒绝服务攻击和端口扫描。
		URL 筛选	旨在监视和控制员工的 Web 冲浪活动，让所有用户安全地访问 Web。
		WildFire	检测并防止未知攻击，且会根据检测结果，在攻击生命周期中自动创建新防护方法，同时不断更新使用的全部技术。
		全球保护	为传统笔记本电脑设备和移动设备的移动用户提供了保护。
		DNS 安全服务	使用预测分析阻止利用 DNS 发动的命令和控制（C2）或数据窃取的攻击。
		Traps 终端保护	为终端提供保护，使其免受旨在运行恶意代码或利用软件漏洞的网络攻击，可防止已知和未知的攻击。
	云和企业安全	VM 系列	下一代防火墙的软件形式，提供了与硬件设备相同的所有安全功能，可以部署在虚拟机管理程序和云上。

业务分类	业务名称	特点描述
云安全	Prisma 访问	一种安全访问服务边缘（SASE）平台，能够将全球各地的移动用户、分支机构和零售店互联并为其提供保护。
	Prisma 公共云	在终端客户的公共云环境中提供全面的可视性和威胁检测。
	Prisma SaaS	一种 SaaS 应用安全产品，能够保护数据，监管数据并确保数据合规，帮助组织安全地采用 SaaS。
未来保护	Cortex 数据池	收集、转换和集成企业的安全数据来高效使用公司提供的安全方案
	Cortex XDR	业界唯一运行完全集成的终端、网络和云数据的检测和响应平台。
	自动聚焦	提供准确的威胁情报，提高调查、防御和响应能力。
	Demisto	借助安全编排、自动化和响应平台，管理警报，标准化流程并自动化第三方产品的操作。
其他服务	支持服务	提供对硬件和软件的持续支持，持续的安全更新，系统升级，错误修复和修复。
	专业服务	直接通过授权的渠道合作伙伴提供专业服务，包括现场人员和远程实践专家，可以根据终端客户的特定要求设计和部署有效的安全解决方案。

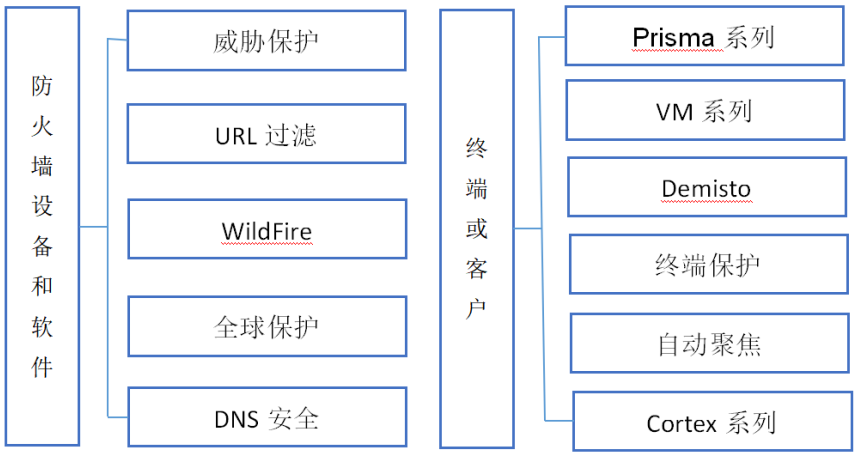
资料来源：公司公告，东兴证券研究所

消费者需要购买下一代防火墙平台，并订阅相关功能，这些**订阅服务通过两种方式出售。**

威胁防护，URL 过滤，WildFire，全球保护和 DNS 安全这些订阅服务作为防火墙平台的可选项出售，与平台绑定；

VM 系列，Traps 终端保护，自动聚焦，Prisma 系列（包括访问、公共云和 SaaS），Cortex 系列（包括 XDR 和数据池）和 Demisto 都是按用户，终端或容量出售的，与用户或终端绑定。

图25：Palo Alto 产品框架图



资料来源：公司公告，东兴证券研究所

4.2.2 大中型客户为主，分销为主要销售模式

公司的终端客户主要是大中型企业，服务提供商和政府机构，客户遍及多个行业，包括教育，能源，金融服务，政府机构，医疗保健，互联网和媒体，制造业，公共部门和电信等。终端客户在各种部署方案中部署公

司的平台来实现各种安全功能。典型的部署方案包括企业边界，企业数据中心和分布式企业边界。终端客户部署通常涉及至少一对公司的产品以及一个或多个订阅，具体取决于终端大小，安全需求以及网络复杂性。

公司主要采取两级间接履行模式通过渠道合作伙伴向终端客户出售产品、订阅和支持产品，将公司的产品、订阅和支持产品出售给分销商，然后再将其出售给经销商，最后将其出售给终端客户。**公司还通过云平台的应用市场将 VM 系列虚拟防火墙直接出售给终端客户**，采取订阅许可模式，如 Amazon 的 AWS Marketplace，Microsoft 的 Azure Marketplace 和 Google 的 Cloud Platform Marketplace。

4.2.3 通过收购增加产品和业务线

Palo Alto 成立于 2005 年，在 2012 成功上市，上市后，公司进行了大量的收购兼并，为公司带了相应的全新产品和业务，为客户提供全面的安全防护。

表9：公司收购情况

时间	被收购公司名称	带来的产品与业务
2014 财年	Cyvera Ltd.	终端软件通过使用一种创新的方法来阻止对终端的未知零日漏洞攻击，从而保护企业免受网络威胁。
	Morta Security, Inc.	提供了一个网络安全专家团队，增强 WildFire 威胁防御产品。
2015 财年	CirroSecure，Inc.	通过为 SaaS 应用程序提供额外的安全性来扩展平台的功能，是新的 Aperture 订阅服务（Prisma SaaS 的前身）的基础。
2017 年 2 月	LightCyber Ltd.	通过添加行为分析来扩展平台功能，是未来新订阅产品的基础。
2018 财年	Evident.io，Inc.	通过添加云服务基础架构保护技术 ，扩展了基于 API 的公共云安全功能。
	Cyber Secdo Ltd.	通过添加终端检测和响应功能（包括独特的数据收集和可视化）来扩展 Traps 的功能以及平台的其他功能。
2018 年 10 月	RedLock	云安全分析技术扩展了平台的公共云安全功能。
2019 年 3 月	Demisto	通过添加 SOAR 产品扩展了平台的功能。
2019 年 6 月	PureSec	无服务器应用程序安全功能扩展了 Prisma 的云安全策略。
2019 年 7 月	Twistlock	容器安全功能扩展了 Prisma 的云安全策略。
2019 年 12 月	Aporeto Inc.	增强 Prisma Cloud 提供的云安全平台的功能。
2020 年 4 月	CloudGenix Inc	增强安全访问服务边缘（“ SASE”）平台。

资料来源：公司历年年报与季报，东兴证券研究所

在 2012 年公司上市之初，公司就有云安全方面的相关业务，虚拟系统升级为大型企业和服务提供商终端客户提供了虚拟化解决方案，实现了大型数据中心，私有云和公有云安全性基础架构。

在 2014 财年（公司的会计年度结束日期为 7 月 31 日，年份采用财年结束时的年份），公司推出采用虚拟形式的防火墙设备，可用于 VMware，Inc.和 Citrix Systems，Inc.的虚拟化平台。

在 2016 财年，公司推出了 VM 系列订阅，它是下一代防火墙的虚拟外形，它既提供永久许可也提供基于期限的订阅服务。VM 系列提供了与硬件设备相同的所有安全功能，但作为软件包可以部署在 VMware 的 ESXi，Microsoft 的 HyperV 和 Red Hat KVM 虚拟机管理程序上，也可以部署在 Amazon 的 AWS 云和 Microsoft 的 Azure 云中。

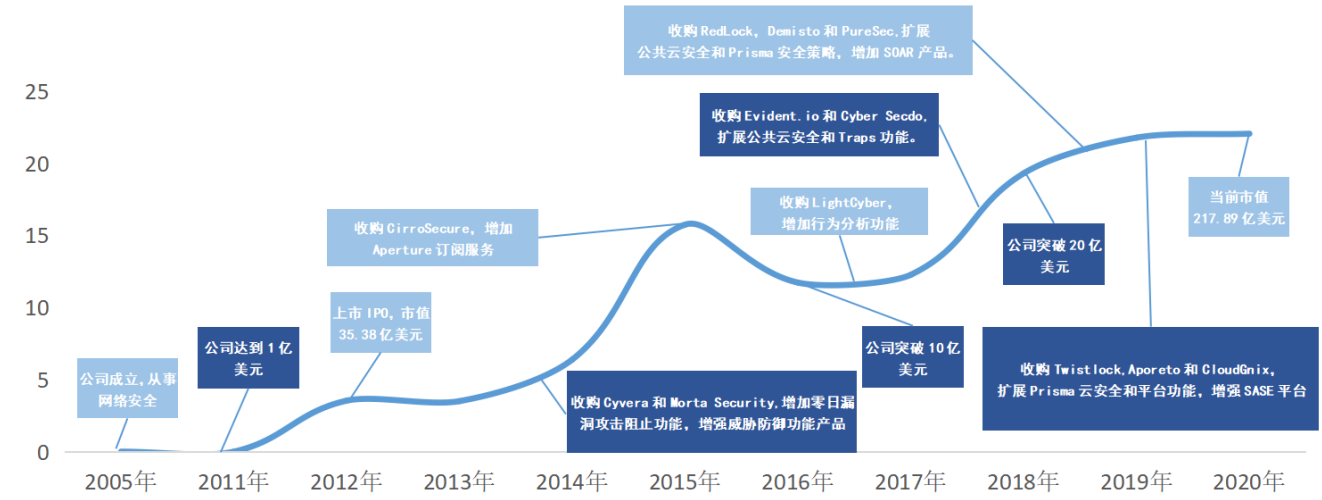
在 2017 财年，公司推出了全球保护（Global Protect）云服务订阅。这项基于云的订阅于 2017 年 9 月发布，使终端客户能够利用下一代安全平台的预防功能来保护远程办公室和移动用户，从而在全球分布的网络和云

环境中提供一致的保护，而无需防火墙设备或远程位置中的软件。有了这个产品，终端客户可以使用公司代表他们运行的基于多租户的基于云的安全基础结构，快速，轻松地添加或删除远程位置和用户，并根据需要建立和调整安全策略。

在 2018 财年，公司推出了 Evident 订阅，这种种基于云的订阅使终端客户能够持续保护公共云基础架构服务，例如云存储。Evident 使终端客户能够持续审计和生成报告，以确保他们能够在公共云中部署应用程序，同时知道云的配置已经满足其系统的安全性和合规性要求。

在 2019 财年，公司推出了 Prisma 云安全产品，Prisma 公有云订阅（以前是 RedLock）确保公有云的安全性和合规性，Prisma Access 订阅（以前是 GlobalProtect 云服务）用于保护用户访问，Prisma SaaS 订阅（以前是 Aperture）用于保护 SaaS 应用程序。除此之外，还有用于在公有和私有云中确保在线网络安全的 VM 系列订阅，用于基于主机的公有云基础设施保护的 Traps，用于保护公有和私有云中的容器的 Twistlock 以及用于保护公有云中的无服务器功能的 PureSec。

图26：Palo Alto 发展历程



资料来源：公司公告，东兴证券研究所

4.2.4 云安全转型，订阅占比不断上升

Palo Alto 的收入由产品收入以及订阅和支持收入构成：产品收入（Product revenue）主要来自设备的销售，还包括软件许可获得的收入；订阅和支持收入（Subscription and support revenue）主要来自订阅和支持产品的销售。

表10：PANW 主要财务数据

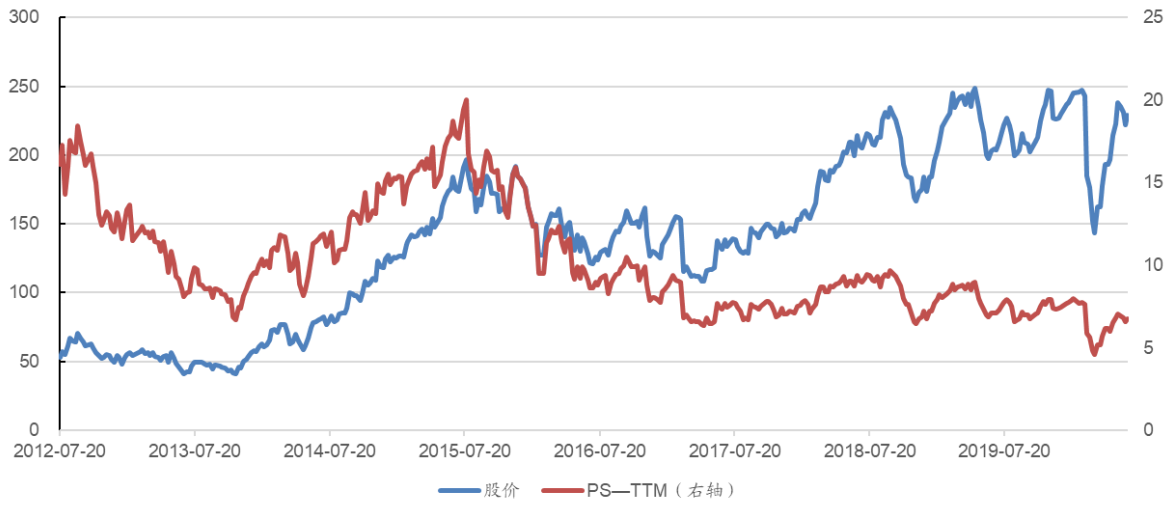
单位：百万美金	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
	07/31/2012	07/31/2013	07/31/2014	07/31/2015	07/31/2016	07/31/2017	07/31/2018	07/31/2019
营收	**255**	**396**	**598**	**928**	**1,379**	**1,762**	**2,273**	**2,900**
YOY	115%	55%	51%	55%	49%	28%	29%	28%
产品收入	**174**	**244**	**340**	**493**	**671**	**709**	**880**	**1,096**
YOY	106%	40%	40%	45%	36%	6%	24%	25%

单位：百万美金	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
	07/31/2012	07/31/2013	07/31/2014	07/31/2015	07/31/2016	07/31/2017	07/31/2018	07/31/2019
订阅和支持收入	**81**	**152**	**258**	**435**	**708**	**1,053**	**1,394**	**1,803**
YOY	139%	89%	69%	69%	63%	49%	32%	29%
其中：订阅收入			**123**	**213**	**357**	**551**	**758**	**1,033**
YOY				73%	68%	54%	38%	36%
订阅收入占比			**21%**	**23%**	**26%**	**31%**	**33%**	**36%**
毛利率	72%	72%	73%	74%	74%	74%	72%	72%
销售占比	45%	50%	56%	56%	56%	52%	48%	46%
研发占比	15%	16%	18%	20%	21%	20%	18%	19%
管理占比	10%	10%	2%	11%	10%	10%	9%	8%
营业利润率	1.5%	-3.8%	-7.9%	-13.0%	-12.9%	-8.1%	-2.6%	-0.2%
经营活动所得现金	77	115	88	350	658	869	1,037	1,056
递延收入	136	249	423	714	1,241	1,774	2,365	2,889
YOY	102%	84%	70%	69%	74%	43%	33%	22%

资料来源：公司财报，东兴证券研究所

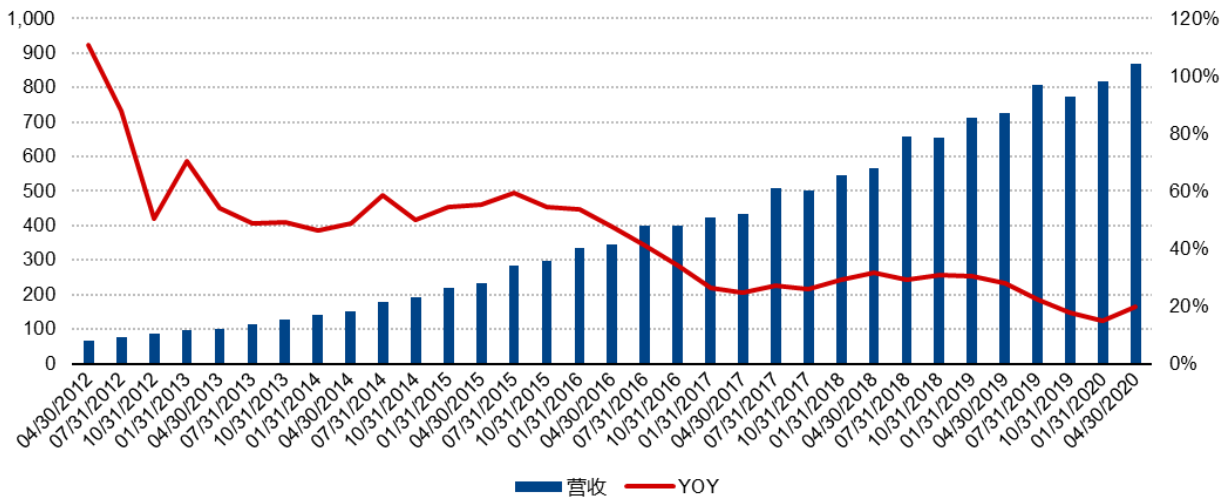
对 SaaS 公司估值基本采用市销率来估值，市销率高低主要取决于收入增速，公司上市后股价与市销率基本保持相同趋势。公司 2013-2015 年公司云安全业务发展迅速，带动公司营收快速增长，增速在 50%以上，公司市销率也随之上升，2015 年 7 月达到最高，接近 20 倍 PS。之后公司市销率随着营收增速的放缓下降，2017 年后公司营收增速逐渐稳定，市盈率也保持较平稳状态。

图27：Palo Alto 估值情况



资料来源：公司公告，东兴证券研究所

图28：Palo Alto 营收情况



资料来源：公司公告，东兴证券研究所

4.3 CrowdStrike 与 Palo Alto Networks 比较

CrowdStrike 成立于 2011 年，一直专注于云安全；而 Palo Alto Networks 成立于 2005 年，一开始专注于防火墙业务，后涉及云安全领域。两家公司在销售模式、收入结构和产品方面存在一定差异。

两家公司虽然市值相近，但是收入规模差距较大，CrowdStrike2020 财年（截止 2020.1.31）营收 4.81 亿美元，同比增长 92.7%，Palo Alto Networks2019 财年（截止 2019.7.31）营收 29 亿美元，同比增长 28%，CrowdStrike 的高估值主要得益于公司业绩的高增长，作为一家云原生安全公司，CrowdStrike 从一开始就采取平台+模块的方式以 SaaS 订阅模式向客户提供服务，符合公有云环境下的用户习惯，实现了用户规模和营收的快速增长。Palo Alto 的特点在于产品齐全，能为各种用户提供全面的安全防护，云安全作为公司安全业务之一起到协同带动作用，发展也相对稳定。

两家公司的共同之处在于跟随公有云的快速发展，推出安全订阅产品，实现公有云安全的突破，从而带动了公司的发展。

表11：CrowdStrike 与 Palo Alto Networks 比较

	CrowdStrike	Palo Alto Networks
成立时间	2011 年	2005 年
市值（2020.6.23）	225 亿美元	221 亿美元
收入规模（2019 年）	4.81 亿美元（YOY：92.7%）	29.00 亿美元（YOY：28%）
PS（TTM）	39.97	6.78
客户	大型组织为主，逐步拓展中小客户	大中型企业，服务提供商和政府机构为主
销售模式	直销为主，通过细分销售团队识别潜在客户，并采用登陆再扩张策略	两级间接履行模式，通过渠道合作伙伴销售，也通过云平台的应用市场销售
收入结构	订阅收入占总收入的 90%以上	产品收入占总收入的 37.8%，订阅和支持收入占总收入的 62.2%，其中订阅占比 36%
产品类型与防护领域	平台+模块化产品，SaaS 订阅集成云模块，包括	以防火墙（包括物理和虚拟设备）为基础，

	CrowdStrike	Palo Alto Networks
	终端安全，安全和 IT 运维（包括漏洞管理）以及威胁情报	提供产品+SaaS 订阅，订阅通过平台和用户两种方式出售，包括企业、云和未来的保护
全产品功能	反病毒、终端检测与响应、USB 设备控制、IT 清洁、漏洞管理、威胁搜寻与情报、恶意软件搜寻与分析	移动用户与分支安全、数据中心与边界保护、威胁检查、自动审查、攻击过程可视化、编排与自动响应、计算安全、网络安全、监管和合规性、云身份识别

资料来源：公司公告，东兴证券研究所

5. 国内安全厂商：全面布局云安全，发力私有云安全和安全运营

与全球信息安全市场相比，中国信息安全行业正处于快速成长期。随着中国信息产业和网络技术的发展，传统的信息安全产品难以满足日益变化的复杂的网络空间，中国的信息安全行业必将向国际看齐，由硬件为主转换为服务为主。前面也提及到，国内公有云安全市场目前尚小且主要被云服务提供商占据，国内安全产商的机遇在私有云和混合云领域。

国内主要的安全厂商都开始全面布局云安全，并将私有云、行业云安全解决方案和安全运营作为发展重点。

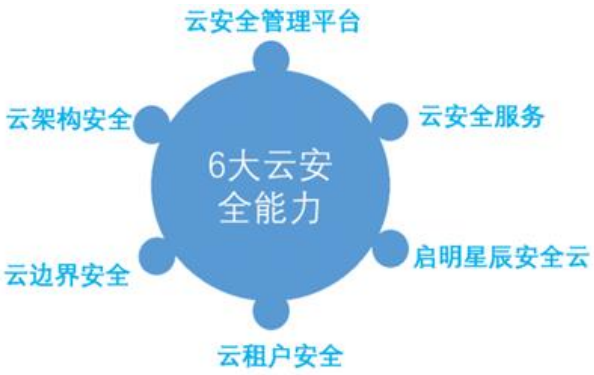
安全厂商通过建设独立的安全运营中心，以专业安全产品和安全服务提供商的身份，直接深入到用户的业务深层，能够更加便捷地获取一线核心运行的信息和数据，更加精准地部署安全策略、应对各种威胁，充分发挥专业队伍的技术和人才优势。对用户而言，这不仅节省了成本，防护效果也大幅提升。对安全厂商来说，安全运营代表着安全产品服务化（SecaaS/SocaaS）的趋势，也代表着类云业务的利润模式，有利于提高客户粘性。

5.1 启明星辰：云安全解决方案全面，前瞻布局城市安全运营

5.1.1 云安全布局全面，收入取得突破

启明星辰针对云安全风险提供六大云安全能力抵御各类风险与威胁，云安全交付模式满足云平台安全和租户个性化安全，同时满足合规要求。

图29：启明星辰提供的六大云安全能力



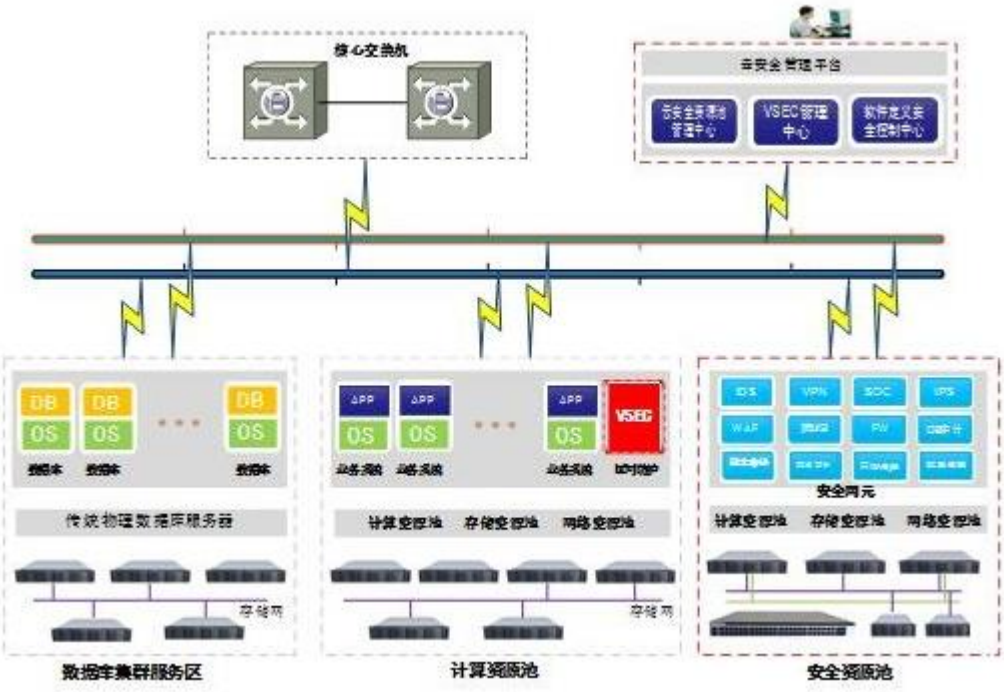
资料来源：公司官网，东兴证券研究所

- 云架构安全即云自身物理环境安全及虚拟环境安全，是云平台整体解决方案基础；

- 云边界安全包括物理网络边界与云内区域边界；
- 云租户安全保障云内业务安全运行，对云上业务提供有效防护；
- 数据安全是云安全的核心，提供数据在云环境下全生命周期安全防护能力；
- 云安全管理平台通过统一安全运营中心管理多地多租户的安全资源，对安全事件和安全风险进行智能分析，感知并发现云内威胁，多维度分析结果，动态关联各项安全能力；
- 云安全服务基于专业化安全分析团队和自动化工具，可为云租户提供云上等保合规咨询、安全检测、安全分析、安全响应及其他应急服务。

公司云安全防护的主要对象为云平台、云租户、云数据和业务系统等。参考等保 2.0 标准规范基本要求及云计算扩展要求，在云平台出口部署防火墙与抗 DDOS 等边界防护产品，实现对南北向流量的拒绝服务攻击防护、访问控制、入侵检测、入侵防御、WAF、防病毒、VPN 和边界隔离等安全防护；在核心交换机旁部署面向多租户的安全资源池，实现对南北向流量的防护、检测与审计，同时对云租户、云数据和业务系统进行防护。其次通过在核心交换机上设置策略路由，将东西流量牵引到安全资源池进行访问控制和安全防护；在租户间使用虚拟防火墙、虚拟 IPS 等网元建立完善的软件定义安全防护链以实现租户间东西向的安全防护，同时对租户云安全资源池中的网元进行深度分析与联动，实现整体闭环体系；最后利用云安全管理平台构建全方位防护体系，建立可视化运维及监控响应体系，满足云计算等级保护要求，实现云安全的集中监测、运维管理、安全服务等能力。

图30：启明星辰云安全解决方案



资料来源：公司官网，东兴证券研究所

公司为中小企业打造的云子可信运用新一代信息技术提高品牌价值，打造云端一体化管理软件，深耕中小企业 SecaaS 市场。云子可信上线两年多，已累计服务中小企业超过 3 万家，用户遍布互联网、教育培训、零售快消、医疗健康、房地产、保险等众多行业和领域。

2019 年，公司通过对大项目的需求跟进，实现了云安全资源池及关联安全管理平台的销售突破，整体云安全的收入达到 1.5 亿元。

表12：启明星辰云安全产品

产品名称	产品功能与特点
云安全资源池	针对私有云或虚拟化资源池用户推出的安全资源池平台，满足用户对虚拟化环境的深度防护和弹性扩展等需求。具有集中管理、快速伸缩性和资源池化三大特点。
云安全管理平台	云安全体系中的上层管理平台系统，可以整合云中各类安全监控资源、采集环境中全量的安全监测信息，集中安全监测、综合安全分析和统一运维支撑等功能，确保云环境与云租户安全。
云 Web 应用审计	数据库审计及防护产品，兼容主流云平台，着重对应用系统操作流程进行梳理，发现异常操作，提供页面仿真回放功能；发现越权行为，核查敏感数据模糊化结果；监测疑似攻击、弱口令、性能瓶颈。
云数据库审计	对云环境中数据库操作的实时审计及防护，可兼容主流云平台，审计数据全面，客观独立，可智能发现异常，适用于主流虚拟环境。
虚拟 WAF	Web 安全防护与应用交付类安全产品，用于防御以 Web 应用程序漏洞为目标的攻击，优化 Web 应用访问，确保 Web 应用安全、快速、可靠地交付。具有 API 防护、恶意注册攻击防护、网站锁防护等特点。
云子可信 SaaS	终端安全 SaaS 云平台，提供 IT 管理和 IT 安全服务，提供全套专业的解决方案，满足于不同的企业的管理需求。具有轻量部署、在线服务和快速上手等优点。

资料来源：公司官网，东兴证券研究所

5.1.2 安全运营发展迅速

公司积极战略布局网络安全新技术，并创新性提出“第三方独立安全运营”新模式，以智慧城市为切入口，前瞻布局城市级安全运营中心。

公司全国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，并已形成成熟的标准化运营体系，未来在持续扩大已有运营中心业务的基础上，将继续向其他二三级城市拓展，2020 年目标力争累计达到 80 个城市的覆盖。

启明星辰北斗安全运营中心面向全国，针对智慧城市建设中的城市云、数据中心、关键信息基础设施及其他政府机构和中小企业提供安全运营中心建设及安全运营服务。**公司 2019 年安全运营与服务收入达 8 亿元，约占公司总收入 20%，同比增长 200%，具备较好成长性和发展前景。**

表13：启明星辰安全运营产品

产品名称	产品功能与特点
基于生命周期的安全业务	基于 Gartner 自适应安全架构的生命周期运营服务，为用户提供一个具备强适应性的智能安全防护体系及全方位闭环安全服务，包括预测、防御、检测、响应等服务。
安全托管业务	针对中小企业需求提供安全托管业务，结合安全专家、运营流程、创新技术和产品为用户提供安全运营服务，帮助用户构建安全运营体系，包括可管理安全设备、安全事件管理与自动化响应等服务。
基于新兴技术和创新模式的安全业务	提供基于大数据、物联网、移动互联网、云计算技术的创新性安全服务，以及基于创新模式的 SEC-aaS 安全即服务、安全众测服务与网络安全保险服务，包括数安全、物联网/工控安全、云安全、移动安全、SEC-aaS、安全众测、网络安全保险等服务。
培训类安全业务	提供安全分析师培养、信息安全意识培训、攻防对抗演练培训、专业认证培训等安全培训服务。

产品名称	产品功能与特点
场景类安全业务	基于不同场景的不同要求，提供场景定制化安全服务，包括重保应急、关保及态势感知、应用安全、合规审计等服务。
设备租赁类业务	提供设备租赁及设备调优服务，为用户提供安全能力保障，节约成本投入。包括安全设备租赁、租赁设备使用培训、租赁设备调优等服务。
咨询顾问类业务	基于用户的组织业务和安全现状，提供安全调研、分析、规划和体系建设等咨询服务，帮助用户建立网络安全体系。包括信息安全规划咨询、信息安全规范咨询、政策合规咨询、安全绩效咨询等服务。

资料来源：公司官网，东兴证券研究所

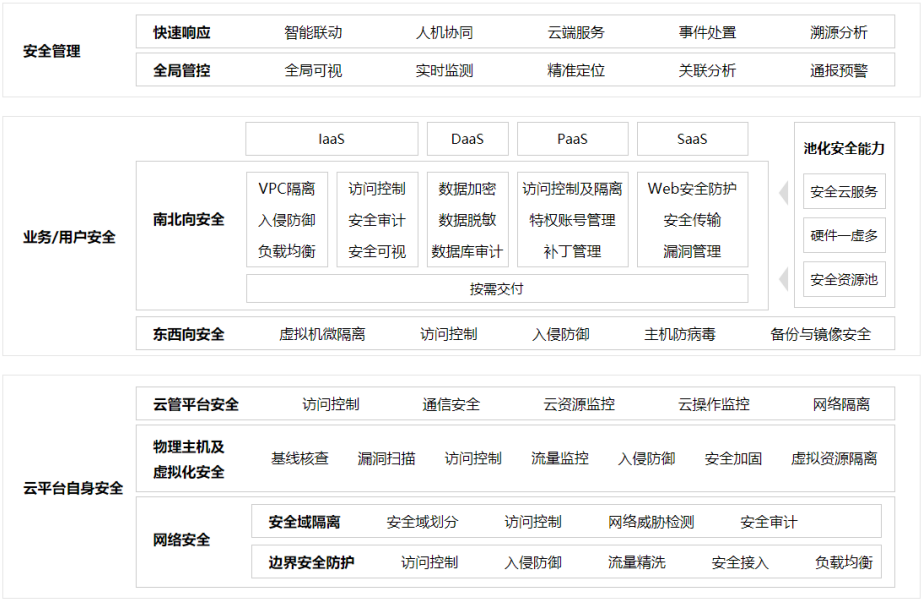
5.2 深信服：云计算与信息安全业务协同发展

公司在发展信息安全业务的基础上，从 2012 年开始布局云计算业务，致力于为各行业用户的数字化转型构筑稳固基石和底座，已初步形成包括桌面云、超融合、软件定义存储、私有云、专属云、混合云的业务布局。**公司云计算业务主要集中于私有云领域，和安全业务下游的客户具有一致性，两块业务有较强的协同效应。**

针对云平台安全合规风险、云用户安全需求难以满足以及云平台缺乏安全全局监测和快速响应能力等云安全挑战，深信服提出了相应的云安全解决方案，从四个方面构筑云安全防护能力。

- **落实平台自身安全合规：**遵照等保 2.0 要求，基于云平台业务特性，从云平台边界安全防护、宿主机及虚拟化安全和云管理平台安全出发，在满足合规的基础上，对云平台提供持续保护。
- **为用户/业务提供安全能力：**为云用户业务系统提供池化的安全资源服务，安全资源池、硬件设备和安全云服务，供用户自行选用和配置安全策略。针对 PaaS/SaaS 等云服务模式，提供基于池化安全资源服务和应用自身的访问控制策略和安全加固措施。
- **统一管理，实现安全全局监测：**在安全运营中心构建网络安全感知平台，帮助云平台运营者实现对云内所有安全事件的全局监测和统一管理。在各业务区部署流量检测探针，实现对云内资产日志及网络流量的统一采集与分析。
- **构建安全事件快速响应能力：**基于网络安全感知平台和联动机制，实现针对安全事件的快速响应，包括可疑 IP 一键封锁，可疑文件一键隔离/查杀，以及安全服务专家进一步的分析定位，快速找出威胁根源，提供修复和加固建议。

图31：深信服云安全方案框架



资料来源：公司官网，东兴证券研究所

表14：深信服云安全产品

产品名称	产品功能与特点
信服云盾	针对专业安全人力资源投入缺乏，融合评估、防护、监测和响应四大模块，帮助用户代管业务安全问题。
信服云眼	为互联网业务提供持续的风险评估、实时监测、篡改处置和应急对抗服务，让用户获得更加安全的保障。
重构入云业务安全边界	针对业务入云后，传统安全机制的失效，搭建深入黑客攻击过程的自适应安全防护平台，提供交付全程可视的安全服务。

资料来源：公司官网，东兴证券研究所

5.3 安恒信息：专注新兴安全领域，“平台+服务”迈向云时代

安恒信息围绕着云计算、大数据及物联网为代表的新一代信息技术，形成了以“新场景”及“新服务”为方向的专业安全平台产品和服务体系。

公司新兴安全业务采取“平台+服务”的模式，平台产品包括云安全平台、大数据安全平台、物联网安全平台等，公司平台产品的收入快速增长，有望催生出安全服务的巨大空间。公司自 2014 年开始陆续推出云安全、大数据安全、态势感知和智慧城市安全等新兴安全领域相关产品和解决方案。2019 年公司网络信息安全平台和服务收入占比已经达到 57%，安全平台产品实现收入 2.72 亿元，同比增长 91.15%，其中云安全平台产品同比增长 176.25%。

5.3.1 安恒信息云安全产品与模式

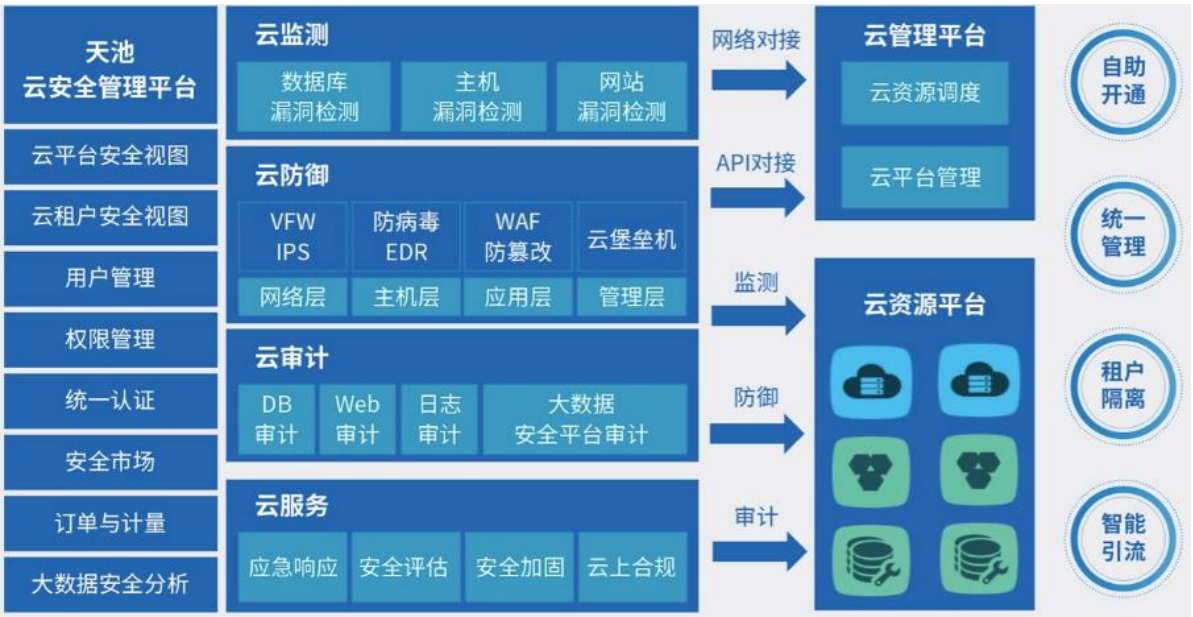
安恒云安全综合解决方案，涵盖公有云、私有云、混合云等不同环境。整体安全建设以云监测、云防御、云审计、云服务为闭环解决思路，全面覆盖云平台网络、主机、计算、存储、业务和管理多个层次，提供给用

户一套合法合规、防护有效、简单易用、灵活扩展的云安全建设方案。平台采用了云端实时网站安全监测与识别技术、云端 DDOS 防护技术、云端 Web 防护技术以及基于机器学习的攻击识别和防护技术。

在私有云领域，公司以天池云安全管理平台作为主要产品，帮助用户构建一个统一管理、弹性扩容、按需分配、安全能力完善的云安全资源池，为用户提供一站式的云安全综合解决方案。

在公有云领域，公司的云安全产品已经上线包括阿里云、腾讯云、华为云、AWS 亚马逊、中国电信天翼云、中国联通沃云等在内的十多家国内外主流公有云平台。

图32：安恒信息天池云安全管理平台框架



资料来源：公司官网，东兴证券研究所

表15：安恒信息云安全产品与服务

产品名称	产品功能与特点
天池云安全管理平台	帮助用户解决云上的安全问题。天池通过不断的汇聚云安全能力，帮助用户构建一个统一管理、弹性扩容、按需分配、安全能力完善的云安全资源池，为用户提供一站式的云安全综合解决方案。
明鉴网站安全监测平台	采用远程监测技术对 Web 应用提供全天候实时安全监测服务，提升网站的安全防护能力和服务质量，通过事件跟踪功能建立安全保障机制，进行以漏洞检测为主的多维度监测，包括安全风险检测(，安全事件监测和网站可用性监测。
玄武盾云防护平台	为私有云提供安全检测、防护、分析、运营等一体化安全防护，事前发现云平台资产，进行安全漏洞检测，事中防护 DDoS、WEB 等安全攻击，避免出现平台瘫痪、黑客入侵、数据泄露等问题，事后通过威胁情报和运营工具进行辅助安全决策。
安恒云（超融合）	集计算虚拟化、网络虚拟化、存储虚拟化、安全功能于一体，提供构建完整的基础设施服务（IaaS）云计算平台方案。可以快速整合基础资源，并按照业务的需要自助分配到各个业务组件当中，为企业客户提供完整的云计算资源的管理平台。
先知云监测服务	提供资产发现、漏洞检测、事件监测和可用性监测等云端 SaaS 服务，可在无感知的情况下发现

产品名称	产品功能与特点
	未知资产，提前发现系统漏洞，实时准确发现入侵事件，发现并关停仿冒系统，诊断系统服务质量，配套全天候安全运营团队。
玄武盾云防护服务	通过威胁情报、DDoS 防护、Web 防护、CC 防护、数据防护 5 大防护模块为用户提供防攻击、防篡改、防瘫痪、防泄露等安全防护，并结合大数据流量处理，对网络安全态势进行数据大屏可视化。
威胁情报服务	提供漏洞情报，安全情报，安全分析报告，活跃黑客组织，攻击类型，被攻击行业等服务。
关键信息基础设施安全监测服务	实时掌握辖区内关键基础设施的网络安全态势网络安全威胁、风险和隐患，监测安全漏洞，掌握网络安全有关情报，及时通报预警重大网络安全威胁，调查、防范和打击网络犯罪行为。

资料来源：公司官网，东兴证券研究所

5.3.2 安恒信息安全运营产品与模式

安恒信息安全平台运营服务基于 AICSO 安全运营平台，剪裁整合包括信息安全管理体系 ISMS、应急响应体系、风险管理体系在内的多个管理体系，融合了传统信息安全服务业务，等级保护要求，实现了安全服务线下能力线上化、专家与产品协作分析数据化、信息安全运营治理工作流程可视化。

AICSO 安全运营平台是以数据和情报驱动，基于自适应安全架构进行环境和态势感知，通过技术、流程、人有机结合完成安全运营，将信息安全服务做到自动化感知、智能分析、应急响应、辅助决策，提供一站式解决方案。并提供云上 SaaS 服务、异地联合运营（SaaS+EPaaS）、本部署运营服务（IaaS+EPaaS+SaaS）三种服务模式。

表16：安恒信息安全运营服务

服务名称	服务功能
运营管理	严密监控、防范大规模扫描行为和网络攻击，实现安全事件的预警、检测、响应、取证。为用户提供运营管理支撑、部分场景运维自动化工具支撑、异地人员能力支撑和项目管理等服务。
安全服务业务	结合专业的安全服务团队为用户提供提供漏洞扫描、安全配置检查、安全设备日志分析、网络架构分析、渗透测试、代码审计、协助加固、回归测试、应急响应、安全培训、安全外包、安全监测等服务。
漏洞管理	漏洞信息采集、漏洞分析、漏洞维度监控展示、漏洞派单及处理结果跟踪、漏洞检查报告、漏洞库。
网络管理能力	自动发现拓扑结构，显示故障、告警信息，网络设备、安全设备等状态信息及端口流量信息。支持对数据库状态信息的采集，提供数据库监控功能，提供图像化呈现。
事件/流量监控	实时监控安全事件，包括事件采集过滤、关联分析、监控大屏。通过采集、过滤、范化日志信息，实现安全事件监控，提供事件显示、进度追踪、安全态势实时监控等功能。
安全风险预警能力	提供安全风险预警能力，基于管理和监控信息与外部威胁情报，进行风险计算，精确分析对网络的影响，可能存在问题的资产进行预警，产生安全响应，查询安全策略及时调动资源降低风险。
应急响应管理能力	提供自适应应急响应机制，基于平台漏洞库、威胁数据库、外部威胁漏洞情报信息及标准的应急响应流程，结合专家团队，实现快速的分析及处置，并持续改进处理结果。

资料来源：公司官网，东兴证券研究所

6. 投资建议

与全球信息安全市场相比，中国信息安全行业正处于快速成长期。传统的信息安全产品难以满足日益变化的复杂的网络空间，中国的信息安全行业必将向国际看齐，由硬件为主转换为服务为主。**国内公有云安全市场**

目前尚小且主要被云服务提供商占据，国内安全产商的机遇在私有云和混合云领域。国内主要的安全厂商都开始全面布局云安全，并将私有云、行业云安全解决方案和安全运营作为发展重点。

推荐公司：云安全解决方案全面，前瞻布局城市安全运营的**启明星辰；**云计算与信息安全业务协同发展的**深信服；**专注新兴安全领域，“平台+服务”快速成长的**安恒信息。**建议关注：山石网科、三六零、绿盟科技等。

表17：推荐公司估值表（截止 2020.06.29）

公司	证券代码	总市值（亿元）	总收入（亿元）	净利润（亿元）	PE			EPS			PB
			19A	19A	19A	20E	21E	19A	20E	21E	19A
启明星辰	002439.SZ	382.58	30.89	6.81	53.36	43.04	32.39	0.77	0.95	1.27	8.79
深信服	300454.SZ	776.25	45.90	7.60	101.52	85.35	68.40	1.90	2.26	2.82	18.26
安恒信息	688023.SH	223.69	9.44	0.92	229.60	162.15	110.38	1.25	1.77	2.60	13.71

资料来源：wind，东兴证券研究所

7. 风险提示

疫情影响下游客户信息安全投入不及预期；政策实施不及预期；市场竞争加剧风险。

相关报告汇总

报告类型	标题	日期
行业深度报告	信息安全行业专题报告之一：从被动防御到主动安全，需求升级驱动信息安全行业高景气	2020-03-28
公司普通报告	深信服（300454.SZ）：安全产品优势领先，云计算业务有望持续超预期	2020-05-11
公司普通报告	安恒信息（688023.SH）：顺应网安产业升级趋势，新兴安全业务有望持续高成长	2020-05-07
公司普通报告	三六零（601360.SH）：政企安全、城市安全将成新的增长极	2020-02-13
行业深度报告	东兴证券信息安全产业洞察：产业增长强势，关注全面型厂商	2019-08-13
公司深度报告	启明星辰（002439.SZ）：安全行业龙头，业绩增长持续性强	2018-03-08

资料来源：东兴证券研究所

分析师简介

王健辉

计算机互联网行业首席分析师，博士，2015 年新财富第二名，2018 年万得金牌分析师第一，2019 年加盟东兴证券计算机团队，组织团队专注研究：云计算、信创网安、医疗信息化、工业软件、AI 大数据、车联网、5G 应用、金融科技及数字货币等领域，奉行产业研究创造价值理念。

研究助理简介

陈晓博

中国人民大学会计硕士，2019 年加入东兴证券研究所，从事计算机行业研究。

分析师承诺

负责本研究报告全部或部分内容的每一位证券分析师，在此申明，本报告的观点、逻辑和论据均为分析师本人研究成果，引用的相关信息和文字均已注明出处。本报告依据公开的信息来源，力求清晰、准确地反映分析师本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与，未来也将不会与本报告中的具体推荐或观点直接或间接相关。

风险提示

本证券研究报告所载的信息、观点、结论等内容仅供投资者决策参考。在任何情况下，本公司证券研究报告均不构成对任何机构和个人的投资建议，市场有风险，投资者在决定投资前，务必要审慎。投资者应自主作出投资决策，自行承担投资风险。

免责声明

本研究报告由东兴证券股份有限公司研究所撰写，东兴证券股份有限公司是具有合法证券投资咨询业务资格的机构。本研究报告中所引用信息均来源于公开资料，我公司对这些信息的准确性和完整性不作任何保证，也不保证所包含的信息和建议不会发生任何变更。我们已力求报告内容的客观、公正，但文中的观点、结论和建议仅供参考，报告中的信息或意见并不构成所述证券的买卖出价或征价，投资者据此做出的任何投资决策与本公司和作者无关。

我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头寸并进行交易，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。本报告版权仅为我公司所有，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、刊发，需注明出处为东兴证券研究所，且不得对本报告进行有悖原意的引用、删节和修改。

本研究报告仅供东兴证券股份有限公司客户和经本公司授权刊载机构的客户使用，未经授权私自刊载研究报告的机构以及其阅读和使用者应慎重使用报告、防止被误导，本公司不承担由于非授权机构私自刊发和非授权客户使用该报告所产生的相关风险和责任。

行业评级体系

公司投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，公司股价相对于同期市场基准指数的表现为标准定义：

强烈推荐：相对强于市场基准指数收益率 15%以上；

推荐：相对强于市场基准指数收益率 5%～15%之间；

中性：相对于市场基准指数收益率介于-5%～+5%之间；

回避：相对弱于市场基准指数收益率 5%以上。

行业投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，行业指数相对于同期市场基准指数的表现为标准定义：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率介于-5%～+5%之间；

看淡：相对弱于市场基准指数收益率 5%以上。

东兴证券研究所

北京
西城区金融大街 5 号新盛大厦 B 座 16 层
邮编：100033
电话：010-66554070
传真：010-66554008

上海
虹口区杨树浦路 248 号瑞丰国际大厦 5 层
邮编：200082
电话：021-25102800
传真：021-25102881

深圳
福田区益田路 6009 号新世界中心 46F
邮编：518038
电话：0755-83239601
传真：0755-23824526