计算机

2021 年 02 月 18 日

云安全专题报告：网络安全的未来在云端

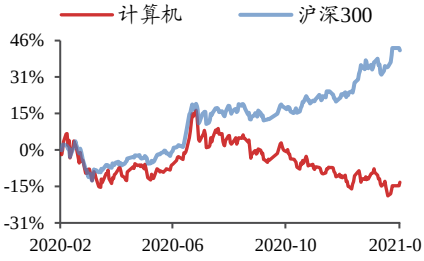
——行业深度报告

陈宝健（分析师）
chenbaojian@kysec.cn
证书编号：S0790520080001

刘逍遥（分析师）
liuxiaoyao@kysec.cn
证书编号：S0790520090001

投资评级：看好（维持）

行业走势图



数据来源：贝格数据

相关研究报告

《行业周报-周观点：密集回购，彰显信心》-2021.2.7

《行业周报-周观点：云计算高景气度持续》-2021.1.31

《行业周报-周观点：继续看好云计算和信息安全》-2021.1.24

● 重点关注网安领域综合实力强，同时在云安全等业务布局领先的厂商

云安全市场伴随着云计算市场的快速发展，及云原生技术的广泛应用而快速增长。国内云安全市场需求旺盛，在新兴云安全技术应用上不断追赶，高速发展可期。建议重点关注网安领域综合实力强，同时在云安全等业务布局领先的厂商，推荐深信服、奇安信、安恒信息、绿盟科技、启明星辰、美亚柏科，其他受益标的包括天融信、山石网科等。

● 云安全市场正处于发展黄金时期，全球市场规模有望达数百亿

一方面，云基础设施的投资不断增加，网络攻击的不断增长，推动云安全市场快速发展；另一方面，云原生技术应用越来越广泛，应运而生的 CASB（云访问安全代理），CSPM（云安全配置管理），CWPP（云工作负载安全防护平台），SASE（安全访问服务边缘模型）等新兴云安全技术快速发展。目前云安全支出占云 IT 支出比例尚处于较低水平。根据 IDC 数据，2020 年全球云安全支出占云 IT 支出比例仅为 1.1%，说明目前云安全支出远远不够，假设这一比例提升至 5%，那么 2020 年全球云安全市场空间可达 53.2 亿美元，2023 年可达 108.9 亿美元。

● 海外云安全市场：技术创新与兼并整合活跃

整体来看，海外云安全市场正处于快速发展阶段，技术创新活跃，兼并整合频繁。一方面，云安全技术创新活跃，并呈现融合发展趋势。例如，综合型安全公司 Palo Alto 的 Prisma 产品线将 CWPP、CSPM 和 CASB 三个云安全技术产品统一融合，提供综合解决方案及 SASE、容器安全、微隔离等一系列云上安全能力。另一方面，新兴的云安全企业快速发展，并获得资本市场的高度认可。同时，传统安全供应商也通过自研+兼并的方式加强云安全布局。例如，Palo Alto Networks 相继收购 Evident.io、RedLock、PureSec 和 Twistlock；McAfee 收购了 Skyhigh。

● 国内云安全市场：市场空间广阔，尚处于技术追随阶段

市场规模上，根据中国信通院数据，2019 年我国云计算整体市场规模达 1334.5 亿元，增速 38.6%。预计 2020-2022 年仍将处于快速增长阶段，到 2023 年市场规模将超过 3754.2 亿元。中性假设下，安全投入占云计算市场规模的 3%-5%，那么 2023 年中国云安全市场规模有望达到 112.6 亿-187.7 亿元。技术发展上，中国在云计算的发展阶段和云原生技术的程度上与海外市场还有一定差距。因此，国内 CWPP 技术应用较为广泛，对于 CASB、CSPM 一些新兴的云安全技术应用较少。但随着国内公有云市场的加速发展，云原生技术的应用越来越广泛，我们认为 CASB、SCPM、SASE 等新兴技术在国内的应用也将越来越广泛。

● 风险提示： 市场竞争加剧风险；技术变革风险；人员流失风险

目 录

图表目录

1、 云安全市场正处于发展黄金时期

1.1、 云基础设施的投资以及网络攻击的不断增长，推动云安全市场快速发展

关于云安全的定义，目前有两种观点：一种是云计算安全，主要是对云自身的安全保护，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；另一种安全云计算，通过使用云的形式提供和交付安全，即通过采用云计算技术来提升安全系统的服务性能，如基于云计算的防病毒技术、挂马检测技术等。我们认为随着云计算的普及，两个概念将实现融合发展的趋势，即以利用云计算的方式为云计算业务提供安全保护。Gartner 在《secure-access-service-edge》报告中论述了类似的观点，即未来云安全将会变成单纯的安全。一方面，云化的基础设施和平台需要安全防护，用传统安全手段赋能云计算；另一方面，云计算的各种新技术、新理念（如软件定义、虚拟化、容器、编排和微服务等），也在深刻变革着当前的安全技术发展路线，因而，未来的云安全，一定会将“云”这个定语去除，等价于安全本身，即安全技术必然覆盖云计算场景，安全技术必然利用云计算技术。考虑到云安全目前所处的发展阶段，本篇报告中我们主要围绕云计算安全（第一种定义）进行讨论。

云安全几乎是伴随着云计算市场而发展起来的，云基础设施投资的快速增长，无疑为云安全发展提供土壤。根据 Gartner 的预测，2021 年全球最终用户在公有云服务上的支出将增长 18.4%，达到 3049 亿美元，高于 2020 年的 2575 亿美元。特别是在 COVID-19 危机之后，转移到云的 IT 支出比例将加速增长。Gartner 预计，到 2024 年，云服务将占全球企业 IT 总支出的 14.2%，远高于 2020 年的 9.1%。

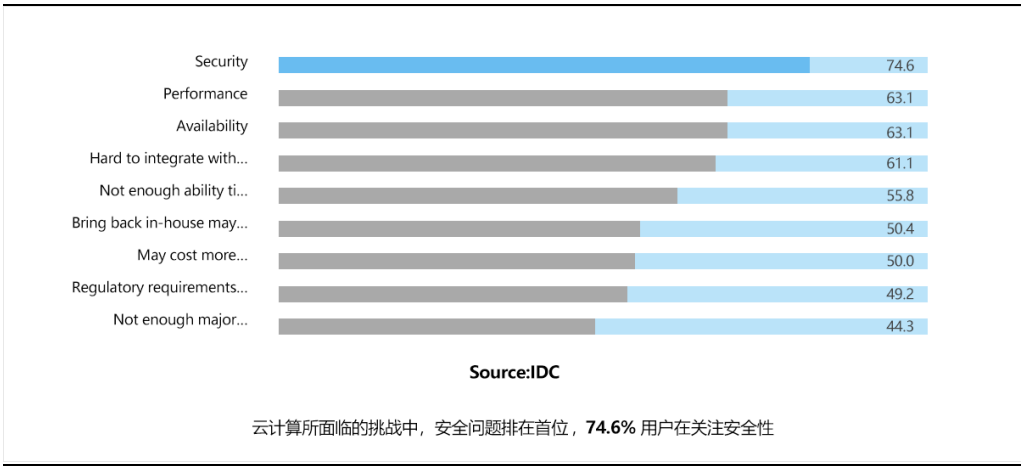
表1：Gartner 预计未来几年全球公有云市场将加速增长（单位：百万美元）

	2019	2020	2021E	2020E
Cloud Business Process Services (BPaaS)	45,212	44,741	47,521	50,336
Cloud Application Infrastructure Services (PaaS)	37,512	43,823	55,486	68,964
Cloud Application Services (SaaS)	102,064	101,480	117,773	138,261
Cloud Management and Security Services	12,836	14,880	17,001	19,934
Cloud System Infrastructure Services (laaS)	44,457	51,421	65,264	82,225
Desktop as a Service (DaaS)	616	1,204	1,945	1,542
Total Market	**242,696**	**257,549**	**304,990**	**362,263**

数据来源：Gartner、开源证券研究所（BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service; Note: Totals may not add up due to rounding）

在云计算发展面临的挑战中，安全和隐私排在了首位。在全球数字化转型的浪潮席卷下，越来越多的企业开始应用云计算技术。资源集中使云平台更容易成为黑客攻击的目标，云上安全问题也更加突出。IDC 调研显示，云计算所面临的挑战中，安全问题排在首位。且 2019 年 RSA 大会上，云安全已跃居热词榜首。

图1：在云计算发展面临的挑战中，安全和隐私排在了首位



资料来源：IDC、深信服

与传统 IT 体系相比，云计算面临着更多的风险点。一是传统安全边界的消失：传统安全以边界为核心，而虚拟化技术使得传统安全边界消失，基于物理安全边界的方式难以在云计算环境下得以应用；

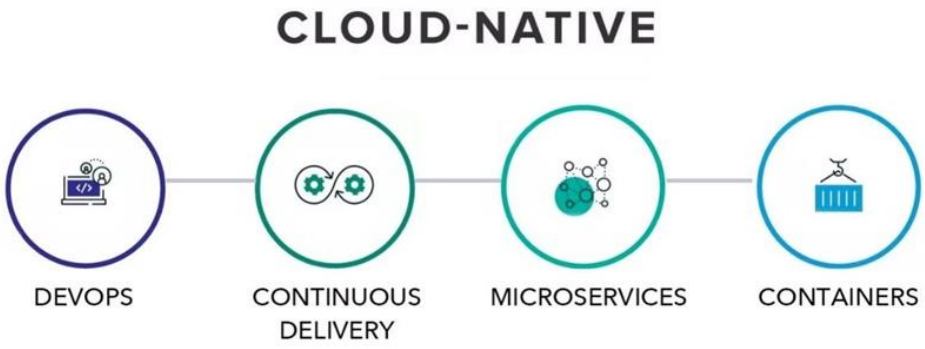
二是用户具有动态性：云计算环境下，用户的数量和分类变化频率高，具有动态性和移动性强的特点，静态的安全防护手段作用被削弱，安全防护措施需要进行动态调整。

三是更高的数据安全保护要求：云计算将资源和数据的所有权、管理权和使用权进行了分离，资源和数据不在本地存储，用户失去了对资源和数据的直接控制，再也不能像传统信息系统那样通过物理控制、逻辑控制、人员控制等手段对数据的访问进行控制。面对用户数据安全保护的迫切诉求和庞大的数据规模，云计算企业需要具有更高的数据安全保护水平和更先进的数据保护手段，以避免数据不可用、数据泄露等风险。

四是多种外部风险：云计算企业搭建云平台时，可能会涉及购买第三方厂商的基础设施、运营商的网络服务等情况。基础设施、网络等都是决定云平台稳定运行的关键因素。因此，第三方厂商和运营商的风险管理能力将影响云计算企业风险事故的发生情况。同时，云计算企业在运营时，可能将数据处理与分析等工作分包给第三方合作企业，分包环节可能存在数据跨境处理、多方责任难界定等风险。

云原生技术逐渐成为云计算市场新趋势，所带来的安全问题更为复杂。以容器、服务网格、微服务等为代表的云原生技术，正在影响各行各业的 IT 基础设施、平台和应用系统，也在渗透到如 IT/OT 融合的工业互联网、IT/CT 融合的 5G、边缘计算等新型基础设施中。随着云原生越来越多的落地应用，其相关的安全风险与威胁也不断的显现出来。Docker/Kubernetes 等服务暴露问题、特斯拉 Kubernetes 集群挖矿事件、Docker Hub 中的容器镜像被“投毒”注入挖矿程序、微软 Azure 安全中心检测到大规模 Kubernetes 挖矿事件、Graboid 蠕虫挖矿传播事件等一系列针对云原生的安全攻击事件层出不穷。

图2：云原生逐渐成为云计算市场新趋势



资料来源：CNCF

CSA 云安全联盟对行业专家进行了一次调查，根据调查问卷结果从 20 个 concerns 中选出最严重的 12 个，包括:数据泄露；身份、凭证和访问管理不足；不安全的接口和应用程序编程接口（API）；系统漏洞；账户劫持；恶意的内部人员；高级持续性威胁（APT）；数据丢失；尽职调查不足；滥用和恶意使用云服务；拒绝服务（DoS）；共享的技术漏洞。

图3：云安全面临的威胁（按照调查结果的严重程度排序）

资料来源：CSA、深信服

云安全责任共担模式在业界已经达成共识。在海外，亚马逊 AWS、微软 Azure 均采用了与用户共担风险的安全策略。对 IaaS 服务来说，云服务提供商（CSP）需保障物理、网络和虚拟化层面的安全，而用户需要保障操作系统、应用程序和数据的

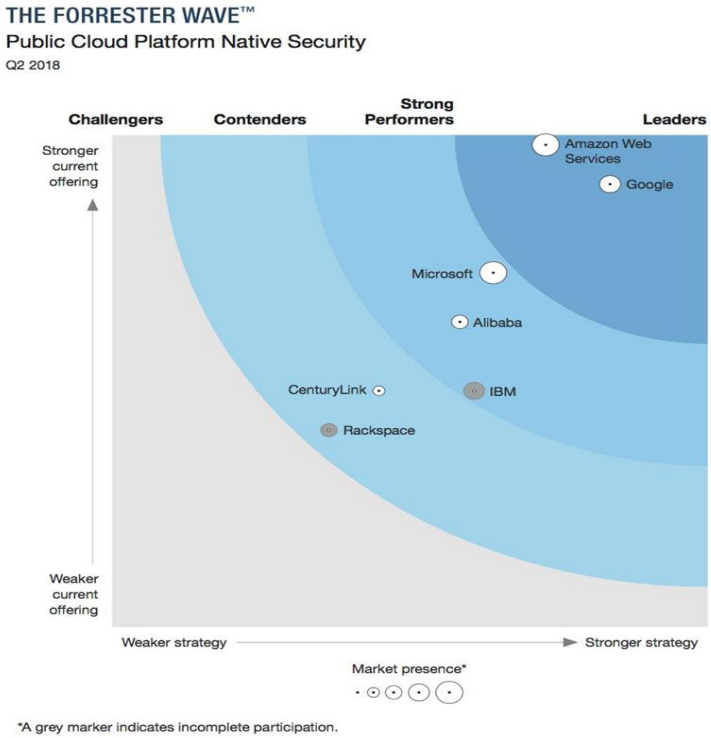
安全；对 PaaS 服务来说，操作系统安全也归 CSP 负责，用户只需要负责应用程序和数据安全；对 SaaS 服务来说， 用户要负责的就是数据安全，而其他所有的部分都是 CSP 的保障范围。近年来云服务提供商(CSP)均在努力提升其安全能力，保护其基础设施和产品安全。

图4：云安全责任共担模式在业界已经达成共识

资料来源：腾讯云

依据责任共担模型，云安全市场的参与者主要分为两类，一类是云服务提供商（CSP）。亚马逊 AWS、微软 Azure、阿里云等云厂商对云基础设施安全的重视程度逐渐提升。

图5：AWS、Azure 等云厂商对云基础设施安全的重视程度高



资料来源：Forrester

以 AWS 为例，AWS 从四个方面对云安全提供了相应的解决方案，包含了 ID 访问控制，检测式控制，基础设置保护和数据保护，为用户提供云上安全。

表2：AWS 从四个方面对云安全提供了相应的解决方案

类别	使用案例	AWS 服务
Identity & Access Management	管理用户访问和加密密钥	AWS Identity & Access Management (IAM)
	云单点登录(SSO)服务	AWS Single Sign-On
	托管的 Microsoft Active Directory	AWS Directory Service
	应用程序身份管理	Amazon Cognito
	轮换、管理和检索密钥	AWS Secrets Manager
	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
	发现、分类和保护您的数据	Amazon Macie
	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	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 Cloud HSM
	预置、管理和部署公有和私有 SSL/TLS 证书	AWS Certificate Manager

资料来源：AWS、开源证券研究所

另一类是专业的安全厂商，主要负责保护用户侧云安全。McAfee、Palo Alto 等老牌的安全厂商不断通过自研+兼并收购完善云安全技术和产品布局；Zscalar、Crowstrike 等新兴安全云厂商迅速发展。

1.2、 CASB、CSPM、SASE 等新技术不断涌现，推动云安全市场创新发展

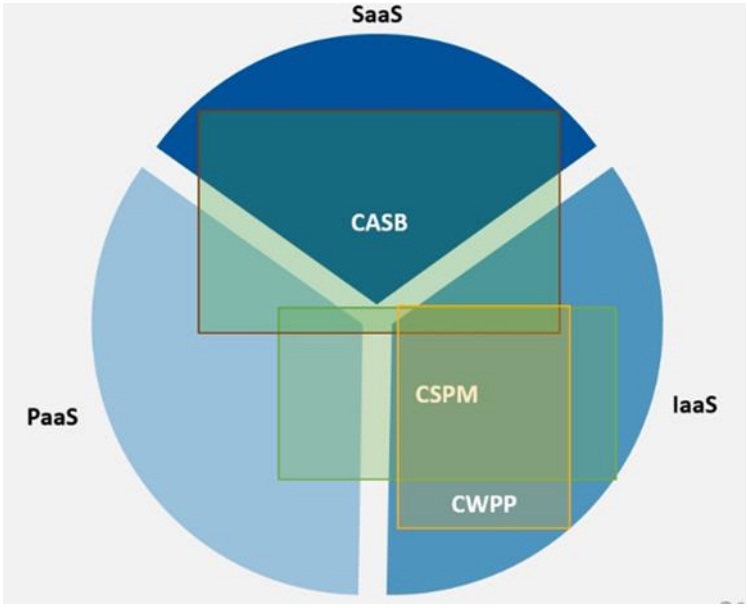
从责任共担模型和云原生两个维度出发，云安全产品可以大体分成三大类：一是传统安全设备的云化。在传统的数据中心中，安全防护通常是通过在安全域入口部署专用的安全设备来实现的，比如防火墙、IDS、IPS 等。在虚拟化的云环境下，传统的安全防护设备不再发挥作用，因此出现了相对应的虚拟防火墙，虚拟 IDS、IPS。

第二类是云服务提供商（CSP）为配套云服务而提供的安全产品，常见的有威胁检测、云数据库安全、API 安全、容器和工作负载安全、用户行为监控、合规与风险管理等。

第三类则是基于云原生应运而生的“新安全”产品和服务，包括 CASB（云访问安全代理），CSPM（云安全配置管理），CWPP（云工作负载安全防护平台），SASE（安全访问服务边缘模型）等。其中，CASB 作为部署在客户和云服务商之间的安全策略控制点，是在访问基于云的资源时企业实施的安全策略。而 CSPM 产品通常使用自动化方式来解决云配置和合规性问题。CWPP 作为一项以主机为中心的解决方

案，主要是满足这些数据中心的工作负载保护需求，因此，主要适用于 IaaS 层。

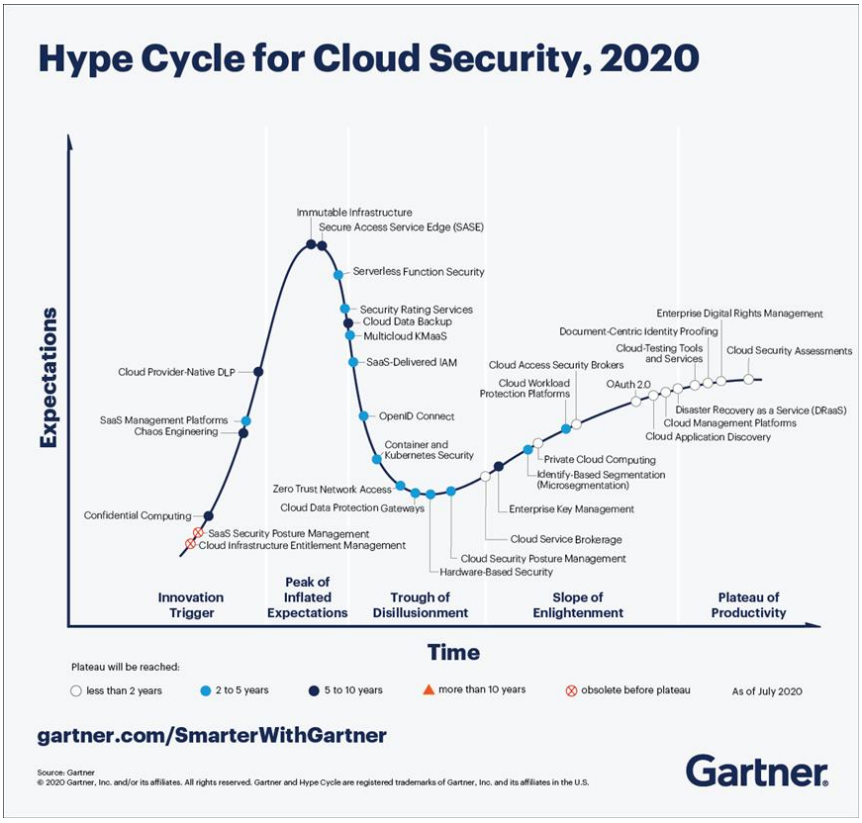
图6：CASB、CSPM、三大云安全工具的覆盖范围关系图



资料来源：安全牛

根据 Gartner 最新发布的《2020 年云安全技术成熟度曲线》，与 2019 年对比，CASB（云访问安全代理），CSPM（云安全配置管理），CWPP（云工作负载安全防护平台），SASE（安全访问服务边缘模型）等新兴技术均实现了快速发展。

图7：Gartner 发布 2020 年云安全技术成熟度曲线

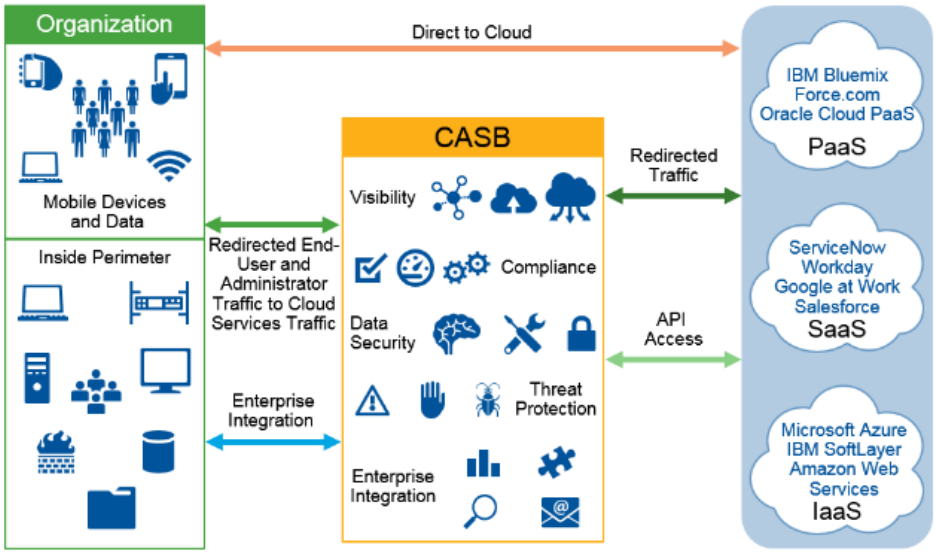


资料来源：Gartner

- **CASB（云访问安全代理）**

Gartner 将云访问安全代理市场定义为解决云服务使用过程安全漏洞问题的产品和服务。CASB 为多云管理提供了一个中心位置，提升对用户活动和敏感数据的细粒度可见性和控制。CASB 相当于一个超级网关，融合了多种类型的安全策略执行点。在这个超级网关上，能够进行认证、单点登录、授权、凭据映射、设备建模、数据安全（内容检测、加密、混淆）、日志管理、告警，甚至恶意代码检测和防护。

图8：CASB 可提升对用户活动和敏感数据的细粒度可见性和控制



资料来源：Gartner

根据 McAfee 官网资料，CASB 核心价值是解决深度可视化、数据安全、威胁防护、合规性这四类问题：

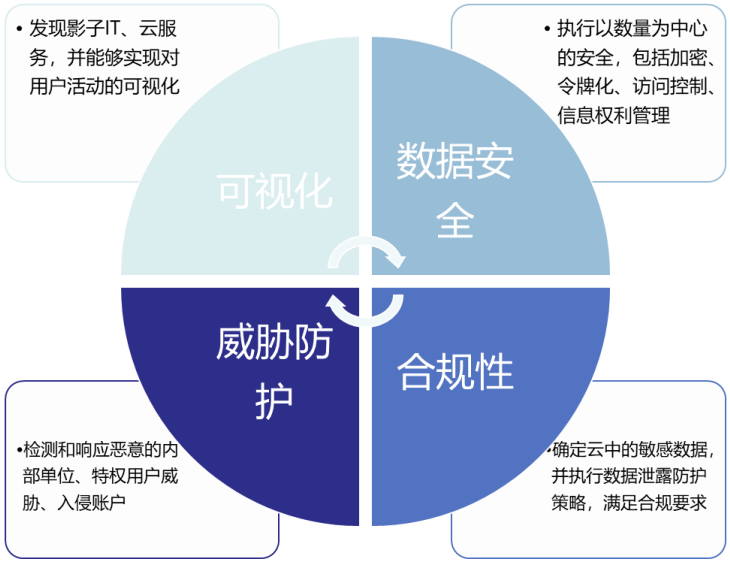
(1) 深度可视化—CASB 提供了影子 IT 发现、组织机构云服务格局的统一视图以及从任何设备或位置访问云服务中数据的用户的详细信息。

(2) 数据安全性—CASB 能够实施以数据为中心的安全策略，以防止基于数据分类、数据发现以及因监控敏感数据访问或提升权限等用户活动而进行有害活动。通常是通过审计、警报、阻止、隔离、删除和只读等控制措施来实施策略。DLP（数据丢失防护）功能很普遍，并且是仅次于可视化的最常用的一项控制措施。

(3) 威胁防护—CASB 通过提供 AAC 来防止有害设备、用户和应用程序版本来访问云服务。可以根据登录期间和登录之后观察到的信号来更改云应用程序功能。CASB 此类功能的其他示例包括通过嵌入式 UEBA 识别异常行为、威胁情报、网络沙箱以及恶意软件识别和缓解。

(4) 合规性—CASB 可帮助组织机构证明，是组织机构在管理云服务的使用情况。CASB 提供了信息来确定云风险偏好并确定云风险承受能力。通过各种可视化、控制和报告功能，CASB 有助于满足数据驻留和法律合规性要求。

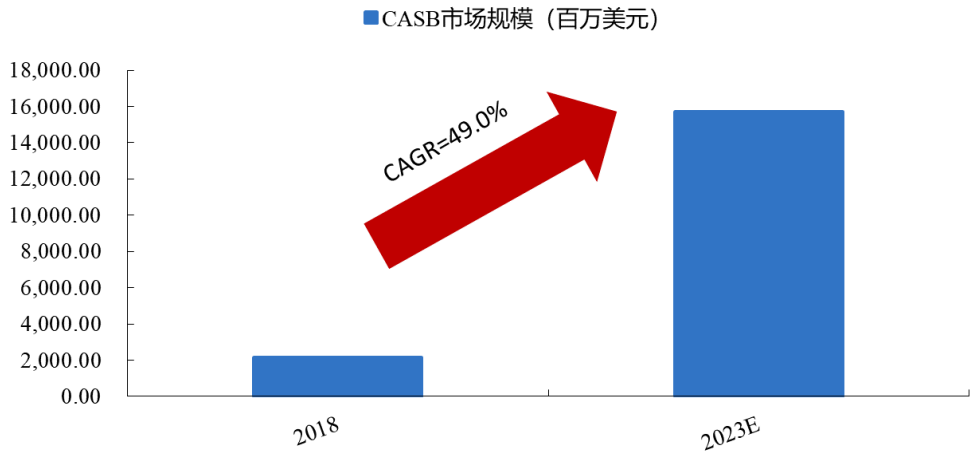
图9：CASB 核心价值是解决深度可视化、数据安全、威胁防护、合规性这四类问题



资料来源：安全牛、开源证券研究所

CASB 市场正处于高速发展阶段。根据 Gartner 预测，到 2022 年，60%的大型企业将使用 CASB，是 2018 年年底使用 CASB 的数量的三倍。而根据 Apps Run The World 预测，全球 CASB 市场规模将从 2018 年 21 亿美元增至 2023 年的 157 亿美元，年复合增长率将达 49.0%。

图10：预计 2018-2023 年全球 CASB 市场复合增长率将达 49.0%



数据来源：Apps Run The World、开源证券研究所

目前，CASB 在云安全市场已经成为一项较为普及的技术，包括 McAfee、Netskope、Symantec、Microsoft、Oracle、Forcepoint、Cisco 在内的知名安全厂商均在 CASB 领域布局。根据 Gartner 发布的 2020 年云访问安全代理（CASB）魔力象限，CASB 市场的主要领导者为 McAfee、Netskope、Microsoft 和 Bitglass。

图11：Gartner 发布 2020 年云访问安全代理（CASB）魔力象限

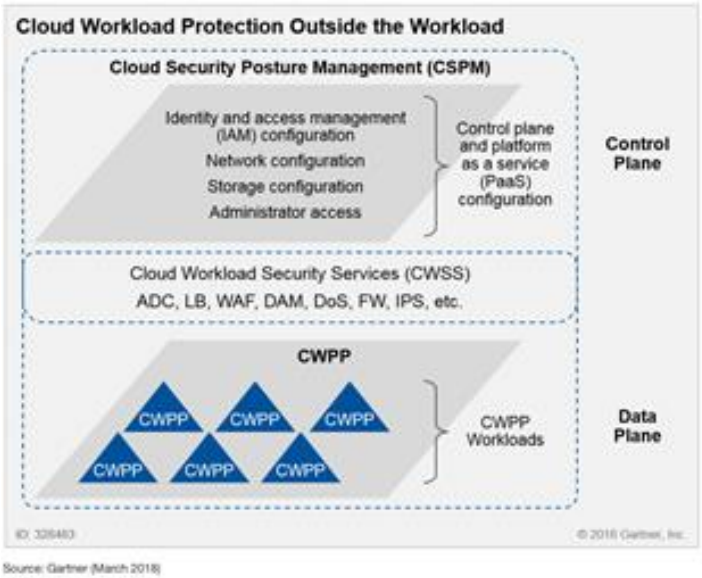
资料来源：Gartner

- **CSPM（云安全配置管理）**

在谈及云工作负载的安全防护的时候，一般分为三个部分去考虑，分属于两个平面。一个是数据平面，一个是控制平面。在数据平面，主要包括针对云工作负载本身进行防护的 CWPP（Cloud Workload Protection Platforms），以及云工作负载之上的 CWSS（云工作负载安全服务）。CWSS 是在云工作负载之上对负载进行安全防护。在控制平面，则都是在负载之上对负载进行防护的措施，就包括了 CSPM，以及前面的 CWSS。

CSPM 能够对 IaaS，以及 PaaS，甚至 SaaS 的控制平面中的基础设施安全配置进行分析与管理。这些安全配置包括账号特权、网络和存储配置、以及安全配置（如加密设置）。理想情况下，如果发现配置不合规，CSPM 会采取行动进行纠偏。

图12：CSPM 可对 IaaS 和 PaaS 云安全配置进行全面、自动化评估



资料来源：Gartner

云安全态势管理(CSPM)四大核心功能：一是可见性。提升云基础架构资产和安全配置的可见性，用户可以跨多云环境和帐户访问单一的来源。配置错误、元数据、网络、安全和更改活动等信息在部署时就会被发现。跨帐户、区域、项目和虚拟网络的安全组策略可以通过单个控制台进行管理。

二是配置分析和管理。CSPM 通过将云应用程序配置与行业和组织基准进行比较，从而消除安全风险并加快交付流程，以便实时识别和纠正违规行为。配置错误、开放 IP 端口、未经授权的修改以及使云资源暴露的其他问题可以通过引导式补救来修复，并提供护栏来帮助开发人员避免错误。存储受到监视，因此始终具有适当的权限，并且数据永远不会意外地向公众开放。此外，还监视数据库实例，以确保启用高可用性、备份和加密。

三是持续威胁检测。CSPM 通过有针对性的威胁识别和管理方法消除多云环境安全警报的噪音，主动检测整个应用程序开发生命周期中的威胁。由于 CSPM 侧重于对手最有可能利用的区域，漏洞根据环境确定优先级，并且无法将易受攻击的代码用于生产，因此警报数量减少。CSPM 还将持续监视环境，通过实时威胁检测来监视环境中的恶意活动、未经授权的活动和对云资源的未经授权的访问。

四是 DevSecOps 集成。CSPM 可减少开销，并消除多云提供商和帐户之间的摩擦和复杂性。云原生、无代理状态管理提供对所有云资源的集中可见性和控制。安全操作和 DevOps 团队获得单一的真相来源，安全团队可以阻止受损资产在应用程序生命周期中取得进展。

根据 Gartner 预测，2019 年，全球 CWPP 市场规模为 12.5 亿美元。预计到 2023 年，这一领域将达到 25 亿美元。

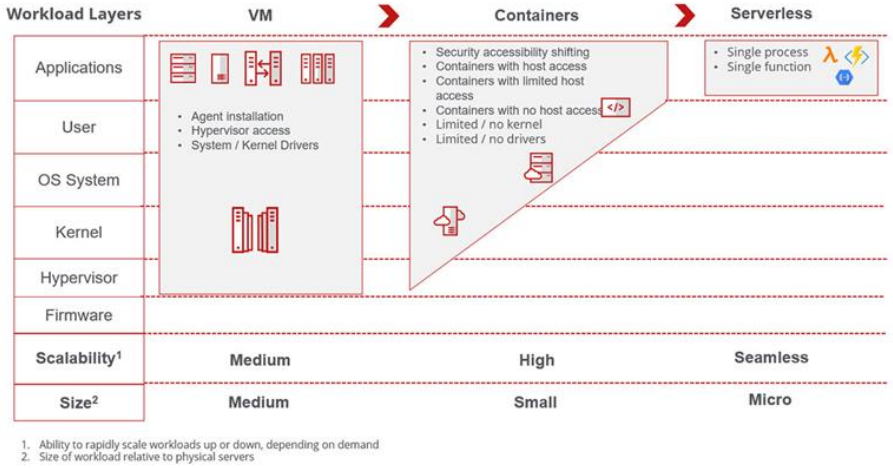
- **云工作负载保护平台（CWPP）**

Gartner 将云工作负载保护平台(CWPP)定义为以工作负载为中心的安全产品，针对现代混合、多云数据中心架构中工作负载的独特保护要求。2016 年，Gartner 首次推出 CWPP 市场指南，旨在为企业用户推荐全球具有代表性的 CWPP 产品提供商。在 2020 年的最新指南中，Gartner 已经将 CWPP 产品扩展为多能力&多平台、脆弱性

扫描&配置与合规、基于身份的隔离&可视和控制能力产品等七大类别，代表厂商也涵盖了全球主流安全厂商。

IT 系统最初的工作负载形式就是物理服务器。随着 IDC 走向虚拟化，工作负载演进为虚拟机形式。云服务中容器成为工作负载的主流，而正在出现和发展的工作负载新形式 Serverless，直接对应用 run-time 虚拟化，改变了传统意义上的服务进程监听-运行模式，是更加精细粒度的瞬态工作负载。随着云计算和云原生需求的发展，云工作负载的形式越来越抽象灵活，同时其部署和运行的生命周期也可越来越短。多种形式和生命周期的云工作负载会长期共存，目前并没出现彼此淘汰的情况，同时这些演进和共存，也使得抽象化定义很有必要。

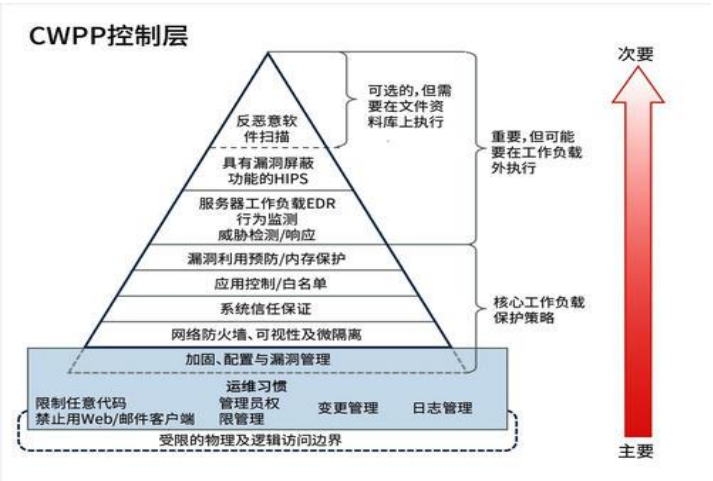
图13：跨工作负载的安全演变



资料来源：McAfee

CWPP 对云上的工作负载，提供多个维度、全方位的保护能力。Gartner 把这种能力分成了 8 大类别（从上到下，重要程度逐层递增），包括：反恶意软件扫描；具有漏洞屏蔽功能的 HIPS；服务器工作负载 EDR 行为监测与威胁检测/响应；漏洞利用预防/内存保护；应用控制/白名单；系统信任保证；网络防火墙、可视性及微隔离；受限的物理及逻辑访问边界。

图14：CWPP 对云上的工作负载，提供多个维度、全方位的保护能力

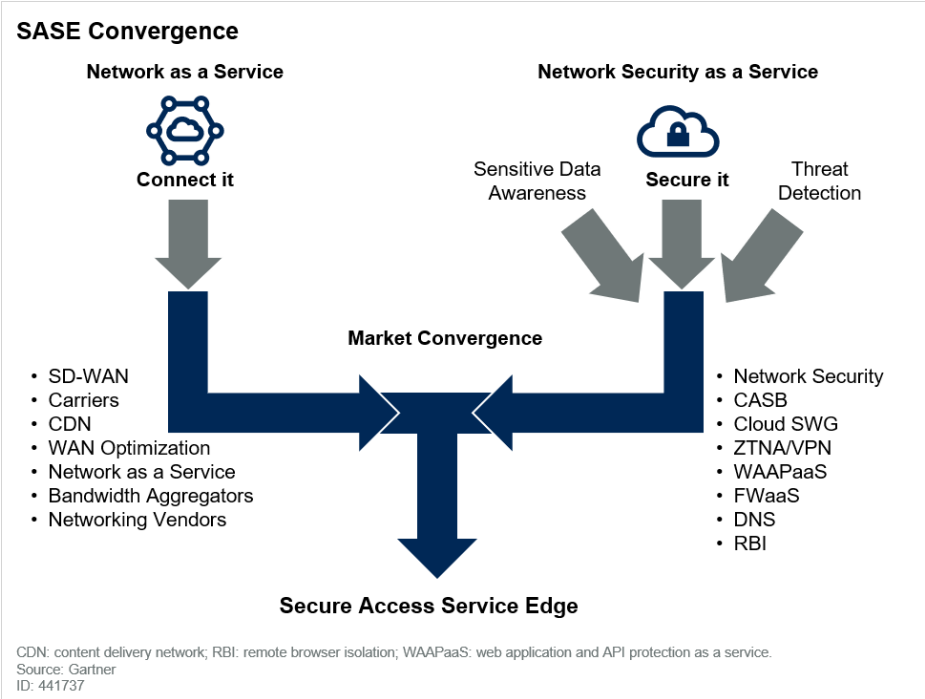


资料来源：Gartner

- **安全服务访问边缘（SASE）**

根据 Gartner 的定义，SASE 是一种基于实体的特性、实时环境、企业安全/合规策略，以及在整个会话中持续评估风险/信任的服务。实体的标识可与人员、人员组（分支办公室）、设备、应用、服务、物联网系统或边缘计算场地相关联。SASE 汇聚网络(例如，SD-WAN)和网络安全服务(例如 SWG、CASB 和 FWaaS)的功能，主要以云服务的方式进行交付。

图15：SASE 汇聚网络和网络安全服务的功能



资料来源：Gartner

根据 Gartner 的定义，SASE 有四个主要特征:

（1）身份驱动

不仅仅是 IP 地址，用户和资源身份决定网络互连体验和访问权限级别。服务质量、路由选择、应用的风险安全控制——所有这些都由与每个网络连接相关联的身份所驱动。采用该方法，公司企业为用户开发一套网络和安全策略，无需考虑设备或地理位置，从而降低运营开销。

（2）云原生架构

SASE 架构利用云的几个主要功能，包括弹性、自适应性、自恢复能力和自维护功能，提供一个可以分摊客户开销以提供最大效率的平台，可很方便地适应新兴业务需求，而且随处可用。

（3）支持所有边缘

SASE 为所有公司资源创建了一个网络——数据中心、分公司、云资源和移动用户。软件定义广域网 (SD-WAN) 设备支持物理边缘，而移动客户端和无客户端浏览器访问连接四处游走的用户。

（4）全球分布

为确保所有网络和安全功能随处可用，并向全部边缘交付尽可能好的体验，SASE 云必须全球分布。因此，Gartner 指出，必须扩展自身覆盖面，向企业边缘交付低延迟服务。

根据 Gartner 预测，到 2024 年，SASE 市场规模将从 2019 年的 19 亿美元攀升至 110 亿美元。同时，到 2024 年，至少 40%的企业将有明确的战略采用 SASE，而在 2018 年年底这一比例不到 1%。SASE 市场已迎来传统 IT 厂商、云计算厂商、安全厂商、CDN 厂商等多方势力的角逐，包括思科、VMware、Palo Alto Networks、Cato Networks、Akamai 和网宿科技等。

1.3、 长期来看，全球云安全市场规模有望达数百亿美元

目前云安全支出占云 IT 支出比例尚处于较低水平。根据 IDC 数据，2020 年全球云安全支出占云 IT 支出比例仅为 1.1%，充分说明目前云安全支出远远不够，假设这一比例提升至 5%，那么 2020 年全球云安全市场空间可达 53.2 亿美元，2023 年可达 108.9 亿美元。

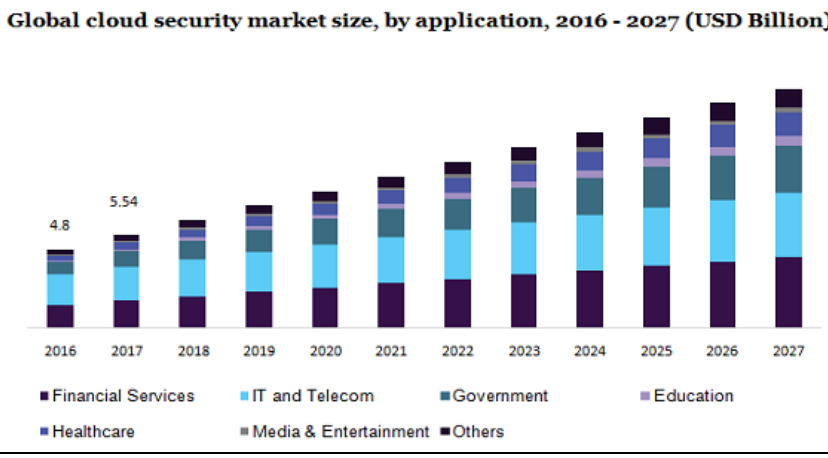
表3：云安全支出占云 IT 支出比例较低

	2020	2023E
Cloud IT Spend		
IaaS and PaaS Vendor Revenue Estimate，IDC	$106.4 Billion	$217.7 Billion
Cloud Security Spend		
Worldwide Hybrid Cloud Security Revenue Eatimate，IDC	$1.2 Billion	$2.0 Billion
Cloud Security Spend as of Cloud IT Spend	1.1%	0.9%

数据来源：IDC、开源证券研究所

云基础设施的投资以及网络攻击的不断增长，将持续推动云安全市场的增长。根据 Million Insights 的最新报告，从 2020 年到 2027 年，全球云安全市场预计将以 14.6％的复合年增长率增长，预计 2027 年全球云安全市场规模将达到 209 亿美元。

图16：2027 年全球云安全市场规模预计将达到 209 亿美元



资料来源：Million Insights

2、 海外云安全市场：技术创新与兼并整合活跃

整体来看，海外云安全市场正处于快速发展阶段，技术创新活跃，兼并整合频繁。一方面，云安全技术创新活跃，并呈现融合发展趋势。例如，综合型安全公司 Palo Alto 的 Prisma 产品线将 CWPP、CSPM 和 CASB 三个云安全技术产品统一融合，提供综合解决方案及 SASE、容器安全、微隔离等一系列云上安全能力。云安全创业公司 Cloud Passage 的云安全解决方案也综合了 CWPP、CSPM 和 CASB 技术，并且结合容器安全防护能力，提供统一云安全防护平台。**另一方面，新兴的云安全企业快速发展，同时，传统安全供应商也通过自研+兼并的方式加强云安全布局**。例如，Palo Alto Networks 相继收购 Evident.io、RedLock、PureSec 和 Twistlock；Check Point 并购 Dome9；McAfee 收购了 Skyhigh。

2.1、 新兴云安全厂商高速成长，并获得资本市场的高度认可

以 Zscaler、Crowstrike、Okta 为代表的新兴云安全厂商不断涌现、高速成长，并且获得资本市场的高速认可。

- **Zscalar：云安全独角兽**

Zscaler 是一家提供云安全服务的美国网络安全公司，成立于 2008 年，共拥有超过 4500 家客户，涵盖 185 个国家，包括福布斯 2000 强中的 450 家企业，客户覆盖金融服务、医疗、制造、航空、运输、消费零售、教育等各个行业。

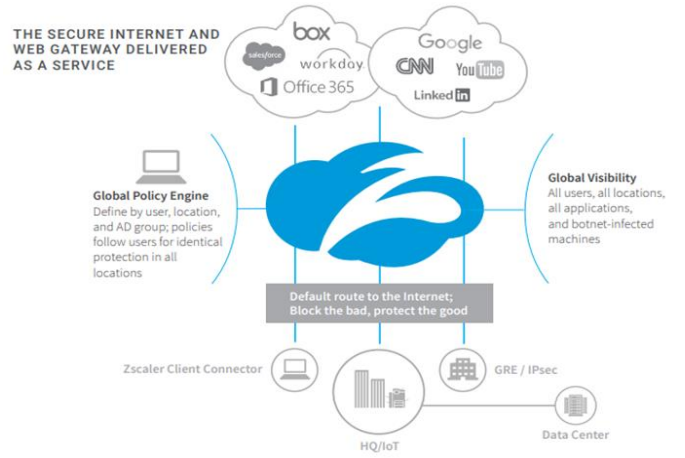
公司四大支柱产品线为：Zscaler Internet Access（ZIA）、Zscaler Private Access（ZPA）、Zscaler Digital Experience（ZDX）和 Workload Segmentation。

图17：Zscaler 拥有四大核心产品线

资料来源：Zscaler 官网

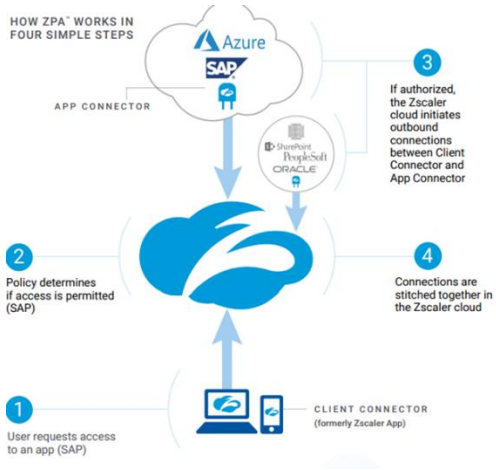
Zscaler 的旗舰产品是 Zscaler Internet Access（ZIA）和 Zscaler Private Access（ZPA）。Zscaler Internet Access 作为用户和提供商之间的中间层，供用户安全连接外部托管的应用。Zscaler Private Access，可供安全访问未托管在第三方云的内部应用。

图18：Zscaler Internet Access 作为用户和提供商之间的中间层，供用户安全连接外部托管的应用



资料来源：Zscaler

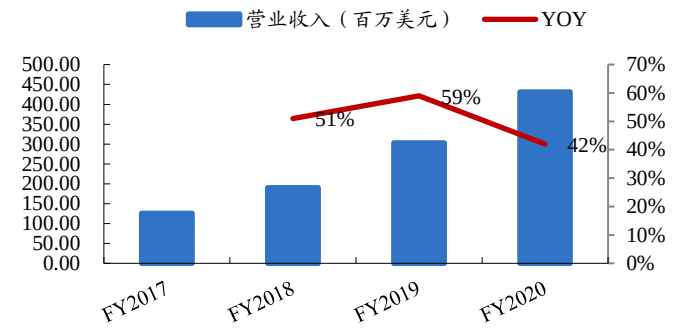
图19：Zscaler Private Access 可供安全访问未托管在第三方云的内部应用



资料来源：Zscaler

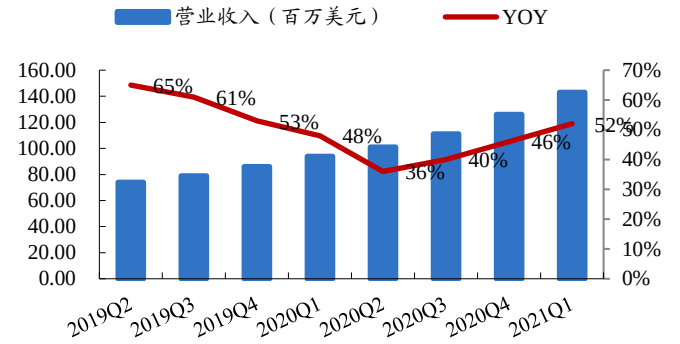
订阅模式下，2017-2020 财年 Zscaler 的收入复合增长率超过 50%。截止 FY21Q1，用户续费率达 122%。

图20：2017-2020 财年 Zscaler 收入复合增长率超过 50%



数据来源：Zscaler、开源证券研究所

图21：2019Q2-2021Q1 Zscaler 收入保持高速增长

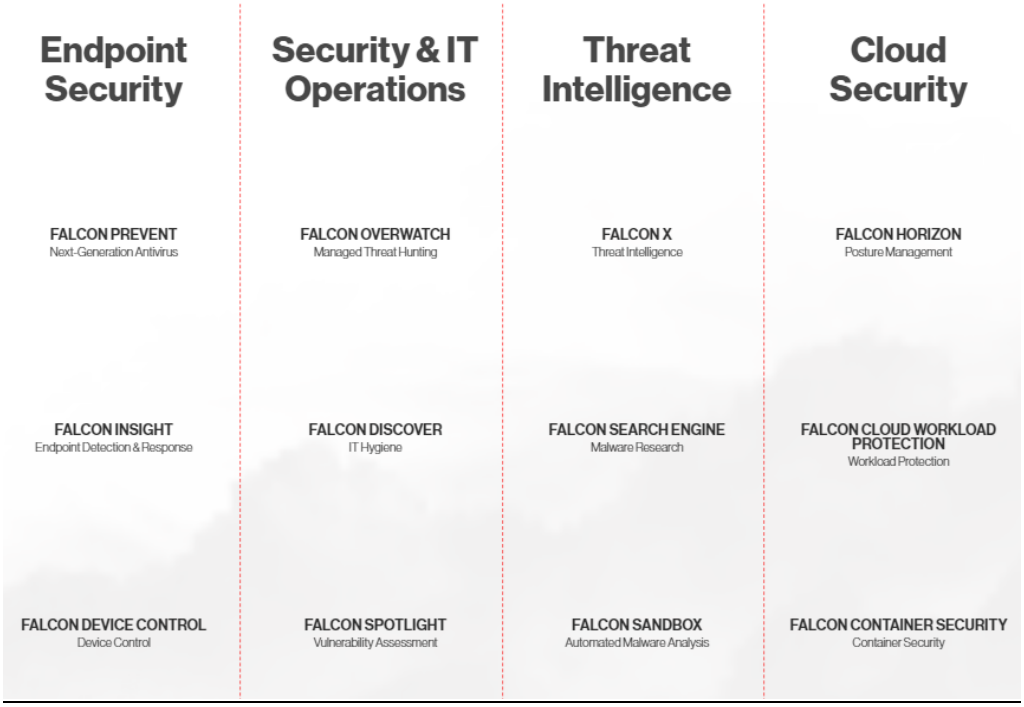


数据来源：Zscaler、开源证券研究所

- **Crowstrike：云交付的下一代终端安全厂商**

CrowdStrike 成立于 2011 年，公司构建了 CrowdStrike Falcon 平台来检测威胁并阻止漏洞。依靠 Falcon 平台，公司创建了第一个多租户云原生的智能安全解决方案，能够保护运行在多个终端的设备。Falcon 平台通过基于 SaaS 订阅模型集成了 11 个云模块，该模型跨越多个安全市场，包括端点安全、安全和 IT 运维（包括漏洞管理）以及威胁情报，以提供全面的漏洞保护。

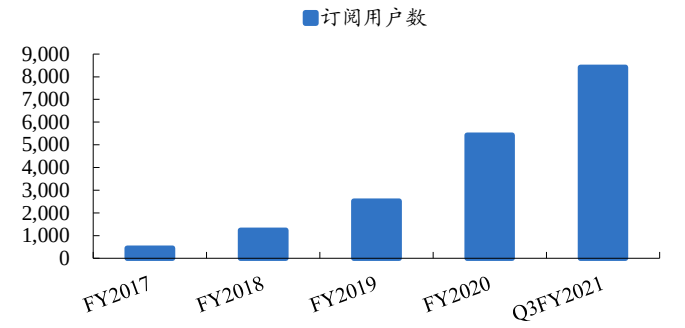
图22：CrowdStrike Falcon 平台的功能模块灵活且可拓展



资料来源：CrowdStrike 官网

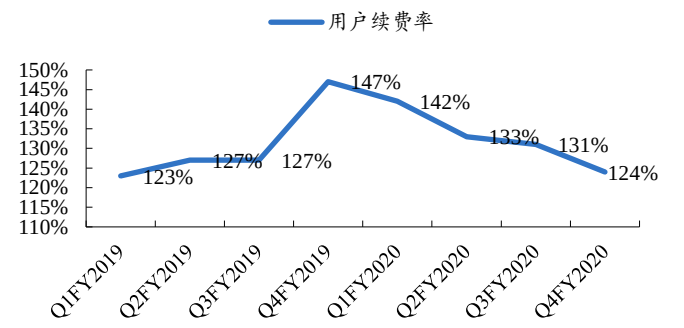
公司用户数量高速增长，同时用户粘性强。从用户数量来看，2017-2020 财年，公司每年的用户数量增长均超过 100%，截止 2021 财年 Q3，公司用户数达到 8416 个，其中覆盖了财富 100 强企业中的 49 家。同时，用户粘性较高，2019 财年至今公司用户续费率基本维持在 120%以上。

图23：CrowdStrike 用户数量高速增长



数据来源：CrowdStrike、开源证券研究所

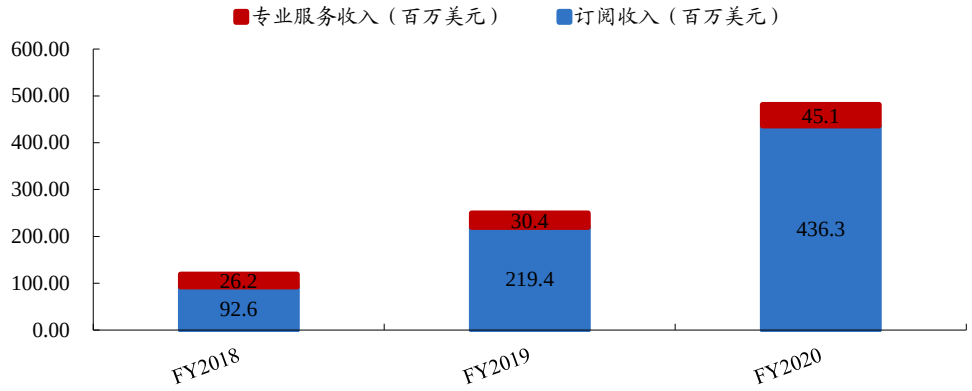
图24：2019 财年至今公司用户续费率基本维持在 120%以上



数据来源：CrowdStrike、开源证券研究所

2018-2020 财年，公司收入的复合增长率超过 100%。公司收入的高速增长，一方面得益于公司所处赛道正在高速增长，客户需求旺盛；另一方面则得益于公司产品的强竞争力。

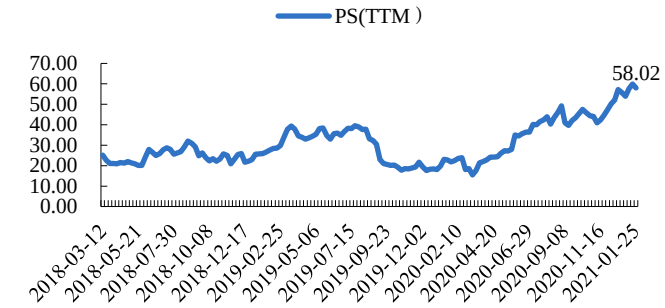
图25：2018-2020 财年 CrowdStrike 收入复合增长率超过 100%



数据来源：CrowdStrike

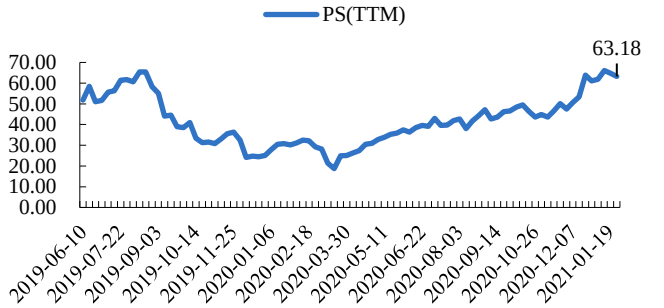
自上市以后，Zscaler 与 CrowdStrike 获得资本市场的高速认可，PS 估值一直处于较高水平。我们认为主要原因有几个方面：（1）赛道。正如前面所述，云安全尚处于高速发展的赛道，随着产品和技术的成熟，市场空间逐渐打开。（2）竞争力。Zscaler 与 CrowdStrike 产品获得用户认可，客户粘性高，客户量与单客户 ARUP 值也在不断提升。因此，过去几年的收入增速保持在较高水平。（3）商业模式。与传统的安全厂商不同，Zscaler 与 CrowdStrike 以云的方式为企业提供安全服务，商业模式也从传统的产品销售模式转变为订阅模式。

图26：自上市以来 Zscaler 的 PS 估值一直处于较高水平



数据来源：Wind、开源证券研究所

图27：自上市以来 CrowdStrike 的 PS 估值一直处于较高水平



数据来源：Wind、开源证券研究所

2.2、传统安全厂商通过自研+兼并，加速布局云安全赛道

以 Palo Alto、McAfee 为代表的传统安全厂商在云安全领域纷纷加速布局，动作不断。

- **Palo Alto：下一代防火墙领导者，加速布局云安全**

Palo Alto 成立于 2005 年，是全球下一代防火墙领导厂商。Palo Alto 下一代防火墙采用 App-ID、User-ID 和 Content-ID 这三种独特的识别技术，针对应用程序、用户和内容实现可视化和控制能力。

图28：Palo Alto 是全球下一代防火墙领导厂商

资料来源：Gartner

近年来 Palo Alto 在云安全领域一直保持高举高打的态势。2018-2020 年，公司相继收购了 Evident.io、Red Lock、 PureSec、Twistlock 和 CloudGenix 等一系列公司，加强在云安全领域的产品和技术布局。

表4：Palo Alto 在云安全领域收购举措频频

	收购标的	金额	业务领域
2018.3	Evident.io	3 亿美元	通过分析服务和帐户配置以应对严格的安全和合规性控制，扩展基于 API 的安全功能
2018.8	Red Lock	1.73 亿美元	支持主流公有云平台的威胁检测服务，可以使用 AI 扫描企业部署找出恶意活动的迹象
2019.5	PureSec	-	以色列无服务器安全平台提供商，PureSec 使其客户能够在可信和安全的计算环境中构建和维护安全可靠的无服务器应用程序
2019.5	Twistlock	4.2 亿美元	容器安全领导厂商，针对云原生应用和工作负载将漏洞管理、合规性和运行时防御相结合
2019.11	Aporeto	1.5 亿美元	致力于提供云安全解决方案，包括分布式防火墙、身份识别代理和特权访问管理的产品
2020.4	CloudGenix	4.2 亿美元	行业领先的云交付 SD-WAN 提供商 CloudGenix
2020.8	Crysis	2.65 亿美元	专注于事件相应、风险管理和数字取证咨询业务
2020.11	Expanse	8 亿美元	开发旨在监控攻击面的解决方案，以便进行风险评估和缓解威胁

资料来源：Palo Alto 官网、安全牛、开源证券研究所

在一系列的收购与整合之后，2019 年 6 月，公司正式推出云安全解决方案 Prisma。Prisma 是唯一在单一平台上以 SaaS 解决方案形式同时提供云安全态势管理和云工作负载保护功能的供应商。Prisma 共包括四大组件：（1）Prisma Access 是安全访问服务边缘（SASE），可以保证企业分支机构和移动用户，无论处于世界任何角落都能在

接入云时受到安全保护。

（2）Prisma Cloud 是统一的云原生安全平台，在混合及多云环境中，为整个云原生技术堆栈、应用和数据提供业界最广泛的安全性和合规性覆盖。2020 年 10 月，Palo Alto 宣布推出包括四个全新云安全模块的 Prisma Cloud 2.0，巩固了其作为业界最全面云原生安全平台（CNSP）的地位。全新的 Palo Alto Networks Prisma Cloud 模块包括：数据安全模块、Web 应用与 API 安全模块、基于身份的微分段模块、身份和访问管理（IAM）安全模块。

（3）Prisma SaaS 为云接入安全代理（CASB），可以实现 SaaS 应用的安全启动。

（4）VM-Series 为 Palo Alto Networks 新一代防火墙，虚拟机箱，可部署于私有及云计算环境中。

图29：Prisma Access 是安全访问服务边缘（SASE）

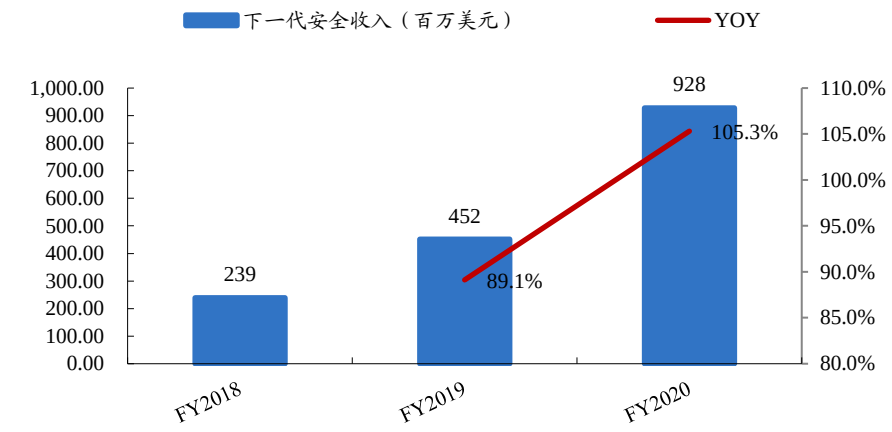
资料来源：Palo Alto

图30：Prisma Cloud 是统一的云原生安全平台

资料来源：Palo Alto

下一代安全产品收入高速增长，在总收入中占比快速提升。Palo Alto 认为下一代安全产品收入是一个关键的财务指标和运营指标，将其定义为 Prisma 和 Cortex 产品及服务收入（含 VM 系列和相关服务在内）。2018 财年，公司下一代安全产品收入占总收入比例仅为 8%，2020 财年这一比例提升至 20%。

图31：Palo Alto 下一代安全产品收入高速增长



数据来源：Palo Alto、开源证券研究所

- **McAfee：云安全能力不断完善**

McAfee MVISION Cloud 已经具备较完整的云安全能力。公司于 2017 年收购了 CASB 厂商 Skyhigh，重新整合成 MVISION Cloud。目前 MVISION Cloud 已扩展到多个类别，包括 CASB，CSPM，CWPP，容器安全性，SSPM 和 SWG。目前 McAfee 成为唯一获得 CASB 2020 Gartner Peer Insights Customer' Choice 荣誉称号的供应商。

表5：MVISION Cloud 已经具备较完整的云安全能力

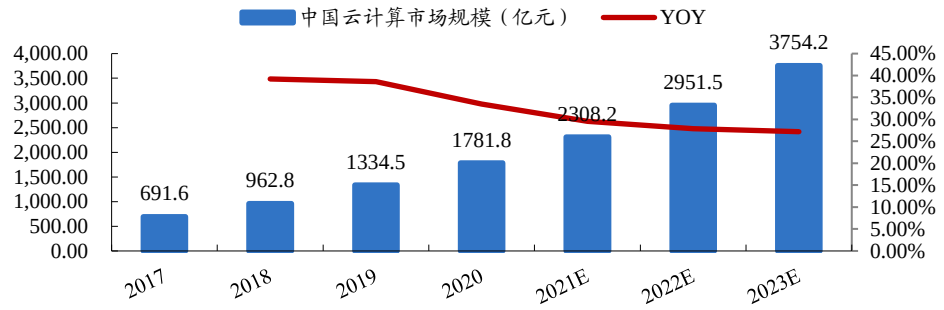
	功能简介
MVISION Unified Cloud Edge	MVISION Unified Cloud Edge 可保护从设备到云的数据，并抵御企业网络不可见的基于 Web 和云原生的威胁。 这是一种实施 Secure Access Service Edge (SASE) 架构的框架，也是一种利用云服务加速数据转型的途径，目的是为了从任何设备访问云和互联网，最终实现员工生产效率的提升。
MVISION CNAPP	MVISION CNAPP 引入了应用程序和数据环境，以独特方式整合适用于公共云基础架构的云安全状况管理 (CSPM) 和云工作负载保护 (CWPP)，进而保护主机和工作负载，包括虚拟机、容器和无服务器功能。
MVISION Cloud	为业务提速的云访问安全代理 (CASB)
Next-gen Secure Web Gateway	McAfee Next-gen Secure Web Gateway 帮助简化安全访问服务边缘 SASE 架构的实现和加速安全云的采用。此外，它还提供了先进的威胁保护、统一的数据控制以及有效支持远程和分布式工作人员的能力。
MVISION Cloud for Container Security	为保护动态和不断变化的容器工作负载及其依赖的基础设施提供了统一的云安全平台及容器优化策略
McAfee Cloud Workload Security	McAfee CWS 可实现对弹性工作负载和容器的发现和防御自动化，从而消除盲点，提供高级威胁防护并简化多云管理
McAfee Virtual Network Security Platform	McAfee vNSP 是一种功能完备的网络威胁和入侵防护系统 (IPS) 解决方案，能够满足私有云、公共云的独特需求

资料来源：McAfee 官网、开源证券研究所

3、 国内云安全市场：市场空间广阔，尚处于技术追随阶段

中国云安全市场空间广阔。根据中国信通院数据，2019 年我国云计算整体市场规模达 1334.5 亿元，增速 38.6%。预计 2020-2022 年仍将处于快速增长阶段，到 2023 年市场规模将超过 3754.2 亿元。中性假设下，安全投入占云计算市场规模的 3%-5%，那么 2023 年中国云安全市场规模有望达到 112.6 亿-187.7 亿元。

图32：预计中国云计算市场仍将处于快速增长阶段

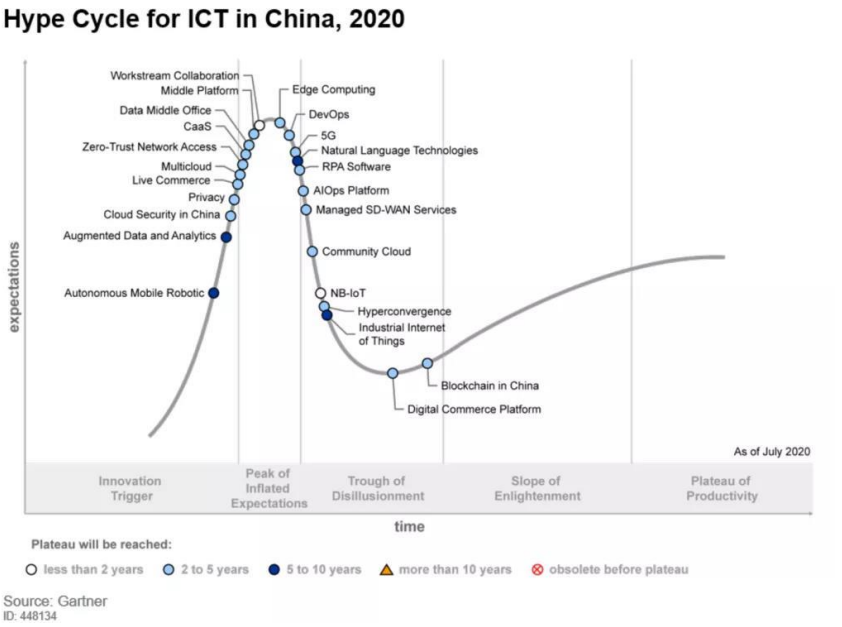


数据来源：中国信通院、开源证券研究所

中国云安全市场尚处于创新发展期。根据 Gartner 发布的《2020 年中国 ICT 技

术成熟度曲线》，其中，云安全在报告中被列入新兴技术范畴。安恒信息、绿盟科技、奇安信、深信服、天融信、启明星辰被列为标杆供应商。

图33：云安全在《2020 年中国 ICT 技术成熟度曲线》报告中被列入新兴技术范畴



资料来源：Gartner（注：中国 ICT 技术成熟度曲线是企业提供评估新技术成熟度的典型工具，为评估新兴数字化技术趋势、技术潜力和商业潜力提供重要依据。横向维度按照技术成熟度分为从新兴到成熟的 5 个阶段，纵向维度表现该技术的期望值。）

中国云安全与海外云安全存在较大的差异。因此，Gartner 特意使用了“中国的云安全”，而非简单的云安全。我们这认为主要由于中国在云计算的发展阶段和云原生技术的程度上与海外市场还有一定差距。**（1）中国私有云市场比公有云市场发展更为领先，对安全资源池等安全机制需求较大。**根据绿盟科技的分析，中国的云计算发展是从虚拟化起步，从私有云到公有行业云，走出了具有中国特色的发展路线。里程碑是开源的 IaaS 项目 Openstack 在国内兴起，国内厂商，如华为、华三、EasyStack 等企业基于 Openstack 研发了各自的云平台，此时国内的云计算需求主要是将硬件服务器虚拟化，再加入多租户管理、网络隔离等需求。通常商用私有云系统是封闭的，缺乏对网络流量按需控制的应用接口，因而，针对这类私有云的安全机制多为安全资源池，通过路由、VLAN 或开放网络接口将流量牵引到资源池进行处理。

（2）从技术应用上来说，中国厂商尚处于追随阶段。Gartner 指出，大多数中国的安全厂商都聚焦在 CWPP 以保护客户云安全。对于一些新兴的云安全技术，CASB 因为国内缺乏重量级的企业级 SaaS 而导致市场较小；CSPM 则因为国内的公有云相比私有云、行业云还是较少，尚未得到重视。但随着国内公有云市场的加速发展，云原生技术的应用越来越广泛，我们认为 CASB、SCPM、SASE 等新兴技术在国内的应用也将越来越广泛。

表6：国内部分安全厂商的云安全产品布局

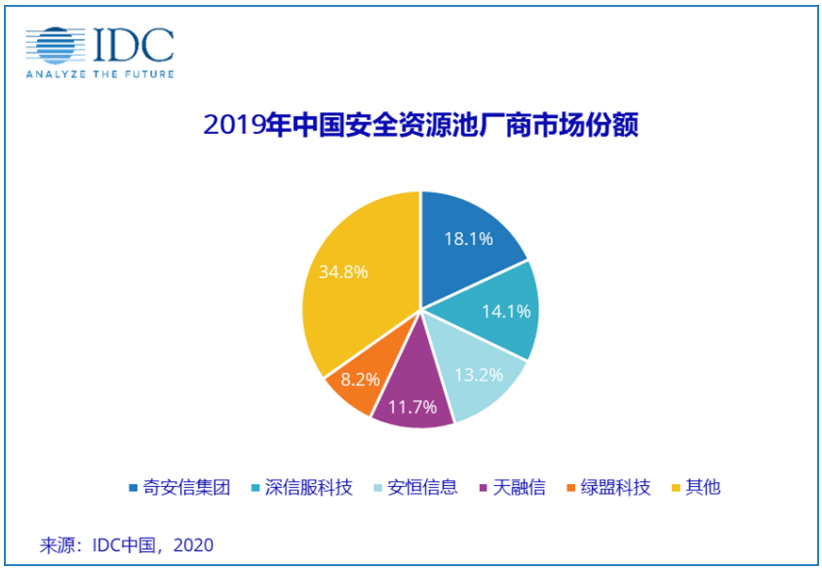
公司	云安全产品名称
奇安信	云安全管理平台、虚拟智慧防火墙、运维安全管理系统（云堡垒机）、统一服务器安全管理系统
深信服	云安全解决方案、信服云眼（网站监测）
安恒信息	云安全平台：安恒云（多云安全与管理平台）、天池云安全管理平台、明鉴网站安全监测平台、玄武盾云防护

公司	云安全产品名称
	平台 **云安全服务**：先知云监测服务、玄武盾云防护服务、威胁情报服务、关键信息基础设施安全监测服务
绿盟科技	容器安全管理系统 NCSS-C、绿盟网站云防护服务 WCP、绿盟黑洞云清洗服务 CCSS、绿盟网站安全监测服务 PAWSS、云安全集中管理系统 NCSS
启明星辰	云安全资源池、云安全管理平台、云 Web 应用审计、云数据库审计、虚拟 WAF、云子可信 SaaS
天融信	虚拟化分布式防火墙、虚拟化安全资源池、终端威胁防御系统
山石网科	山石云·格（微隔离）、山石云·界、山石云·集、山石云·池（云安全资源池方案）
安全狗（美亚柏科参股子公司）	**云安全 SaaS 服务**：日志分析及态势感知云服务、Web 应用安全云服务、网页防篡改云服务、(云)主机安全云服务、抗 DDOS 云服务、7*24 小时安全专家服务、安全云主机 **私有云安全产品**：云垒·立体式私有云安全纵深防御平台、云眼·新一代(云)主机入侵监测及安全管理系统、云隙·自适应微隔离系统、云甲·容器自适应安全管理系统、啸天·安全大数据态势感知系统、云固·新一代网页防篡改系统、云御·新一代网站应用防御系统、云网·补丁管理系统

资料来源：各公司官网、开源证券研究所

国内应用较为广泛的云产品为以安全资源池为核心的云安全管理平台。云安全资源池提供虚拟化的安全能力，如防火墙、WAF、IDS、IPS、堡垒机、数据库审计等，并通过统一安全管理平台对各类安全能力进行组织和编排，形成整体安全方案。在这样的架构下，云上流量不需要集中引至同一区域进行集中处理，通过边缘就近防御的方式降低安全业务带来的网络时延。同时，运营商通常具有多供应商云平台，对不同云平台的适配和对接也逐渐成为行业标配。根据 IDC 报告，2019 年中国安全资源池市场的规模达到 7960 万美元，同比增长 78.3%，市场正以强劲的发展趋势快速扩张，占领部分安全解决方案市场，奇安信、深信服、安恒信息、天融信、绿盟科技市场份额领先。

图34：国内安全资源池市场中奇安信、深信服、安恒信息等市场份额领先



资料来源：IDC 中国

在新兴云安全技术中，CWPP 在国内的应用相对比较成熟。在国际权威咨询机构 Gartner 发布的《云工作负载保护平台市场指南》中，腾讯云主机安全、阿里云云安全中心、山石云·格（CloudHive）入选 Gartner CWPP 全球市场指南。Gartner 从企业用户视角，对云上负载平台的保障需求进行了全面的市场风险分析和处置建议，

并以多能力&多平台能力、脆弱性扫描&配置与合规能力、基于身份的分段&可视化与控制能力、应用控制/预期状态执行能力、服务器 EDR&负载行为监控与威胁监测/响应能力、容器与 K8S 保障能力、无服务器保障能力七大能力矩阵为企业用户推荐全球具有代表性的 CWPP 服务提供商。阿里云和腾讯云入围“全功能、多系统”的全球供应商，山石网科的微隔离可视化云安全产品——山石云·格（CloudHive）成功入选指南中“基于身份的分段&可视化与控制能力”分类。

图35：阿里云云安全中心入选 Gartner CWPP 全球市场指南


Table 1: Broad, Multi-OS Capabilities

Vendor	Product, Service or Solution Name
Alibaba Cloud	Server Guard
[illegible]	AtomicWP Workload Protection
[illegible]	GravityZone Platform

Gartner, Inc. | 716192

Page 12/24

资料来源：阿里云云栖号

图36：山石网科进入 Gartner CWPP 全球市场指南


《Market Guide for Cloud Workload Protection Platforms》 Published 14 April 2020

Table 3: Identity-Based Segmentation, Visibility and Control Capabilities

Gartner

ColorTokens	Xshield
Edgewise	Zero Trust Auto-Segmentation for Hybrid Cloud
Guardicore	Centra
Hillstone Networks	CloudHive
Illumio	Adaptive Security Platform (ASP)
Palo Alto Networks (acquired Aporeto)	Prisma Cloud
TrueFort	TrueFort
ShieldX (container-based)	ShieldX Elastic Security Platform

资料来源：山石网科公众号

SASE 在国内市场均处于新风口。2020 年 9 月 10 日，深信服基于多年的云安全研究技术及安全产品研发能力重磅发布 SASE 安全产品“云安全访问服务 Sangfor Access”，标志着深信服将全面进入安全能力的云化交付时代。云安全访问服务的主要三大服务为 SIA、SPA 和 SAP，这三大服务集结多个安全模块，为用户提供从上网安全管理、业务安全接入到大数据威胁分析的全方位安全保障。

服务一：Sangfor Internet Access（SIA）

聚焦上网安全服务，可解决上网侧，包括对终端、SaaS 应用进行访问的安全问题。通过 SD-WAN 接入服务引流实现流量上云，搭配身份认证、恶意 URL 过滤与流量管理、数据泄密管控、终端安全、安全智能防火墙等安全模块对流量进行管理，从而在用户终端与互联网/应用服务之间隔离出一块安全缓冲区，建立企业安全建设的新防线。

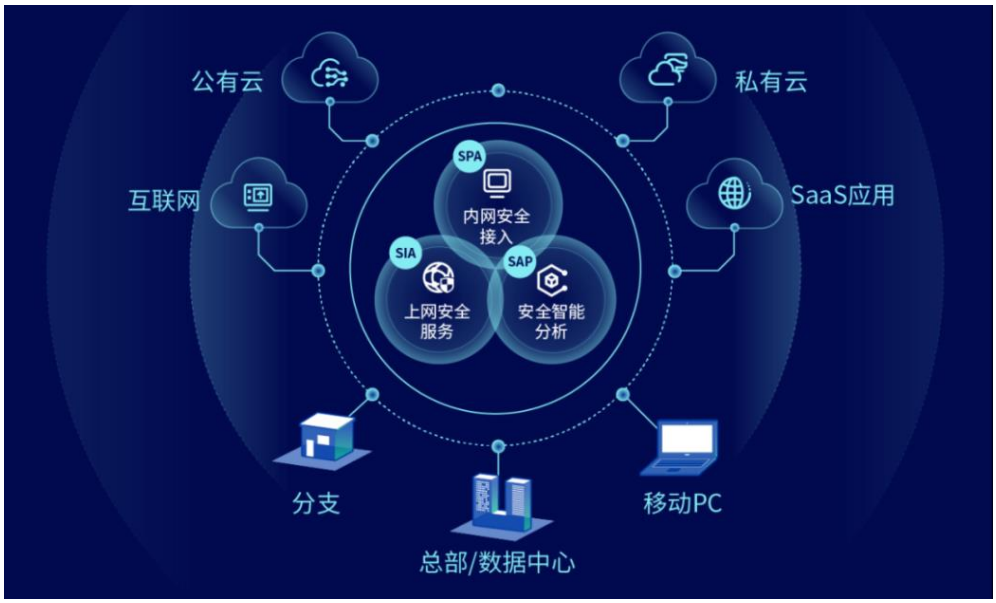
服务二：Sangfor Private Access（SPA）

聚焦内网接入安全服务，可解决私有数据中心访问的安全问题。提供基于 SDP 的云 VPN 接入，基于身份的权限控制、认证等模块，确保企业员工、合作伙伴在任何地方任何时间通过全球各地 POP 点网络访问业务时更安全、更隐私、更稳定的访问体验。

服务三：Sangfor Analytics Platform（SAP）

聚焦安全智能分析服务，可解决端到端访问的安全风险分析问题。通过大数据、人工智能、UEBA 等技术手段或模型分析安全风险，并启动威胁预警，帮助企业建立云端大数据分析平台，实现端到端访问时企业数据资产、安全威胁可视可预警。

图37：深信服云安全访问服务是一个以 SASE 模型为核心的安全服务平台



资料来源：深信服官网

4、 投资建议

云安全市场伴随着云计算市场的快速发展，及云原生技术的广泛应用而快速增长。目前云安全支出占云 IT 支出比例尚处于较低水平，长期来看全球市场规模有望达数百亿美元。国内云安全市场需求旺盛，在新兴云安全技术应用上不断追赶，高速发展可期。建议关注网安领域综合实力强，同时在云安全等新安全业务布局领先的厂商，推荐深信服、奇安信、安恒信息、绿盟科技、启明星辰、美亚柏科，其他受益标的包括天融信、山石网科等。

表7：建议关注网安领域综合实力强，同时在云安全等新安全业务布局领先的厂商（截止 2021.2.18 收盘）

证券代码	公司简称	当前市值（亿元）	归母净利润（亿元）			PE			PS			
			2020E	2021E	2022E	2020E	2021E	2022E	2020E	2021E	2022E	评级
300454.SZ	深信服	1305	8.03	10.84	14.60	164	122	90	24	17	13	买入
688561.SH	奇安信	733	-3.28	0.06	4.85	-223	12901	151	17	13	10	买入
688023.SH	安恒信息	190	1.37	1.91	2.56	138	99	74	14	10	8	买入
002439.SZ	启明星辰	292	8.54	11.09	14.02	34	26	21	7	6	5	买入
300369.SZ	绿盟科技	102	3.05	4.30	5.82	33	24	18	5	3	3	买入
002212.SZ	天融信	226	5.70	7.97	10.77	40	28	21	-	-	-	-
300188.SZ	美亚柏科	148	4.08	5.33	6.67	36	28	22	6	4	4	买入
688030.SH	山石网科	61	1.07	1.37	1.74	40	28	21	7	5	4	-

数据来源：Wind、开源证券研究所（天融信、山石网科盈利预测均来源于 Wind 一致预期）

5、 风险提示

市场竞争加剧风险；技术变革风险；人员流失风险

特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。
因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

分析师承诺

负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及开源证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5%～20%；
	中性（Neutral）	预计相对市场表现在－5%～＋5%之间波动；
	减持	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡	预计行业弱于整体市场表现。
备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。		

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的机构或个人客户（以下简称“客户”）使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于机密材料，只有开源证券客户才能参考或使用，如接收人并非开源证券客户，请及时退回并删除。

本报告是基于本公司认为可靠的已公开信息，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的开源证券网站以外的地址或超级链接，开源证券不对其内容负责。本报告提供这些地址或超级链接的目的纯粹是为了客户使用方便，链接网站的内容不构成本报告的任何部分，客户需自行承担浏览这些网站的费用或风险。

开源证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。开源证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

开源证券研究所

上海
地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼10层
邮编：200120
邮箱：research@kysec.cn

深圳
地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层
邮编：518000
邮箱：research@kysec.cn

北京
地址：北京市西城区西直门外大街18号金贸大厦C2座16层
邮编：100044
邮箱：research@kysec.cn

西安
地址：西安市高新区锦业路1号都市之门B座5层
邮编：710065
邮箱：research@kysec.cn