头豹 LeadLeo

FROST & SULLIVAN 沙利文

2021年
中国安全托管服务市场报告

2021 China Managed Security Service Market Overview

2021年中国マネージドセキュリティ市場報告

报告标签：安全托管、安全运维、主动防御、安全即服务、事件响应

供应商

头豹研究院
弗若斯特沙利文咨询（中国）

报告说明

沙利文及头豹研究院谨此发布中国云安全系列报告之《2021年中国安全托管服务市场报告》。本报告旨在分析中国安全托管服务特点、市场环境、技术动向及发展趋势，并分析中国安全托管服务市场竞争格局，判断在中国安全托管市场处于领袖梯队和挑战者梯队的供应商及其差异化竞争特点。2021年第一季度，沙利文联合头豹研究院对安全托管服务市场进行了下游用户体验调查。受访者来自泛互联网、金融、医疗、教育、制造、能源、物流等多个领域，用户所在公司规模不一，细分市场有别。

本报告最终对市场排名、领袖梯队、挑战者梯队的判断仅适用于本年度中国安全托管服务市场发展阶段。

本报告所有图、表、文字中的数据均源自弗若斯特沙利文咨询（中国）及头豹研究院调查，数据均采用四舍五入，小数计一位。

报告摘要

中小企业需求加速安全托管服务落地

安全管理外包服务在运维成本、服务弹性等维度上占据优势，其主要客户群体以价格敏感度较高的中小企业为主。中国安全托管服务仍处于起步阶段，庞大的中小企业安全运维需求将推动安全托管服务普及。

提供一站式运营管理，提高企业综合安全防御

安全托管服务供应商向客户提供一站式运营管理服务以提高企业综合安全防御，有效解决安全产品部署及运维难题；涵盖企业IT与云资产评估、风险监测、漏洞扫描、安全监控及应急响应等主要服务。

快速识别攻击、游戏行业安全需求持续释放

中国游戏行业是DDoS流量攻击的重灾区，安全托管服务可提供专业安全专家技术支持，快速识别攻击类型，缩减检测及响应周期，从而减少中小游戏公司用户流失及数据泄露。2020年疫情推动游戏行业网络安全需求释放，加速安全托管服务应用落地。

无监督学习与ATD

无监督学习通过聚类算法有效解决安全数据膨胀及信息杂乱等数据标注难的问题；在云上及传统MSS应用领域，无监督学习主要应用于ATD系统集成，实现快速及智能威胁识别。

目录

Contents

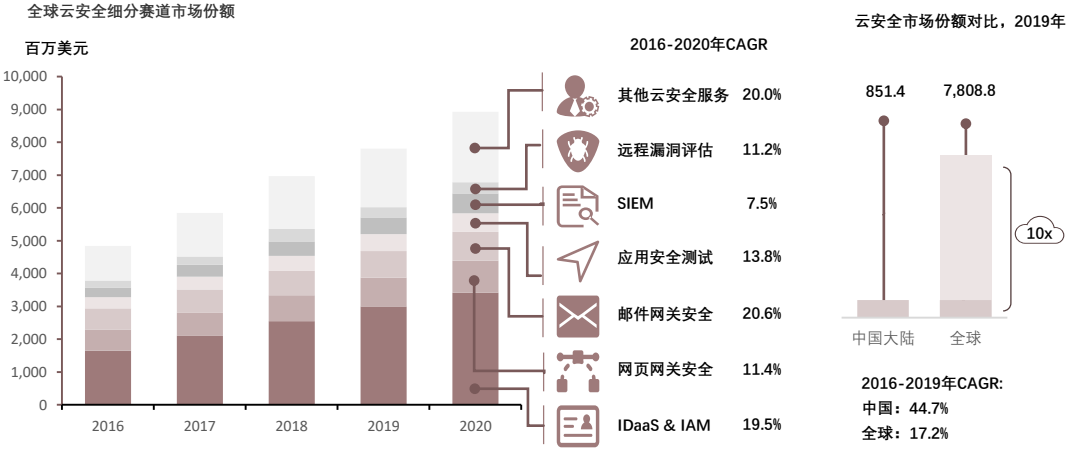
Chapter 1
市场综述

- **中国安全托管市场简述：**
  - 市场现况简述
- **安全托管基础能力：**
  - 监控与扫描
  - 应急响应与安全辅助
  - 定制化服务能力

中国安全托管服务市场综述——市场现况简述

2020年，中国云安全托管服务处于初步发展阶段，但伴随云安全需求释放及SOAR等MSSP运维技术迭代升级，传统MSSP业务加速向云端架构转型

全球云安全细分赛道市场份额及区域对比（百万美元），2016-2020年



- **MSSP从传统驻场安全托管运维服务转向云安全托管服务，实现云端虚拟架构安全漏洞持续监控、风险事件应急响应、快速处置**

2020年，云计算、大数据、物联网及人工智能技术驱动下，企业数字化程度逐渐提升。企业信息安全防御关口逐步前移，从被动防御转向主动防御；同时，安全即服务风潮持续推动下，中国网络安全商业模式实现从“产品”到“产品+服务”模式转型。得益于SIEM、SOAR等网络安全产品及技术迭代及云计算需求释放，MSSP从传统驻场安全托管运维服务向云端虚拟化运维服务转型。与传统网络安全托管服务相比，云安全托管服务供应商通过云上安全监管、云扫描、云清洗等运维服务实现安全风险事件快速响应、数据泄露及安全漏洞持续监控，确保企业客户关键业务数据资产在多云之间安全状态的一致性及无缝性。

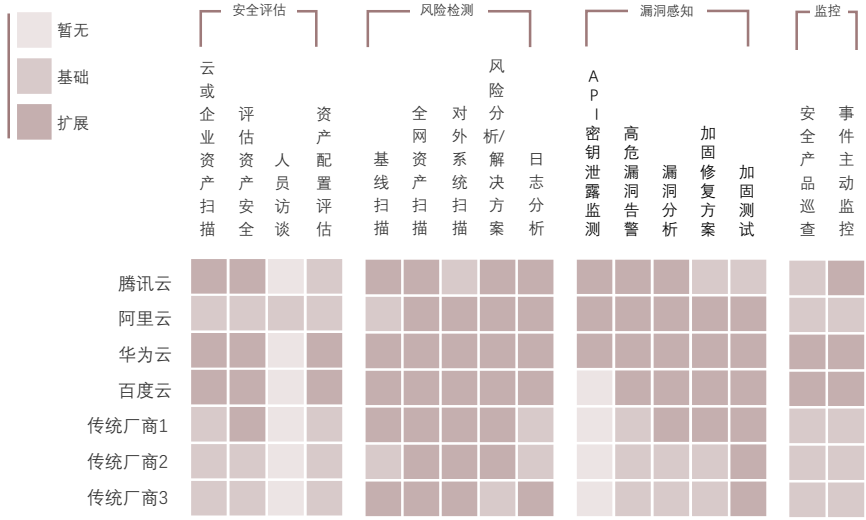
伴随中国社会数字化转型，大量企业将业务迁移至云端。但由于上云企业的IT环境转变为混合云、多云的架构，其环境复杂性大幅提升，导致网络安全暴露面加大，云安全需求持续释放。2016年后，全球云端安全监控、SIEM、远程漏洞评估等云安全细分市场持续扩容，2016年至2020年平均年复合增长率超过15%。纵观全球云安全市场，中国云安全市场体量较大，占全球市场1/10。未来中国云SIEM、远程漏洞管理等市场扩容，有望推动云安全托管服务行业向规模化、标准化、智能化发展。

中国安全托管服务基础能力——监控与扫描

MSSP可向企业客户提供一站式安全运营管理服务以提高企业综合安全防御力；扫描及监控服务模块集中对资产重要度、漏洞严重度、网络暴露面进行综合梳理及实时监控

安全托管供应商服务及相关基础能力对比（一）

监控与扫描模块



- **安全托管服务供应商可向客户提供一站式安全运营管理服务，基础服务可分为监控与扫描、响应及处置、定制化服务能力三大模块**

网络安全产品及技术日趋细化，导致部分企业客户难以根据自身需求准确选择网络安全产品，进而阻碍了企业对现有网络安全架构的运维、防控及优化；而安全托管服务供应商通过SOC（安全运营中心）向企业客户提供一站式安全监控及运营管理服务以提高企业综合安全防御，有效解决安全产品部署及运维难题；根据安全托管服务的子服务类型分类，安全托管服务基础服务可分为（1）监控与扫描、（2）响应及处置、（3）扩展服务能力三大模块。

- **监控与扫描模块侧重于针对企业IT资产重要度、漏洞严重度、网络暴露面等多维度进行综合梳理及实时监控**

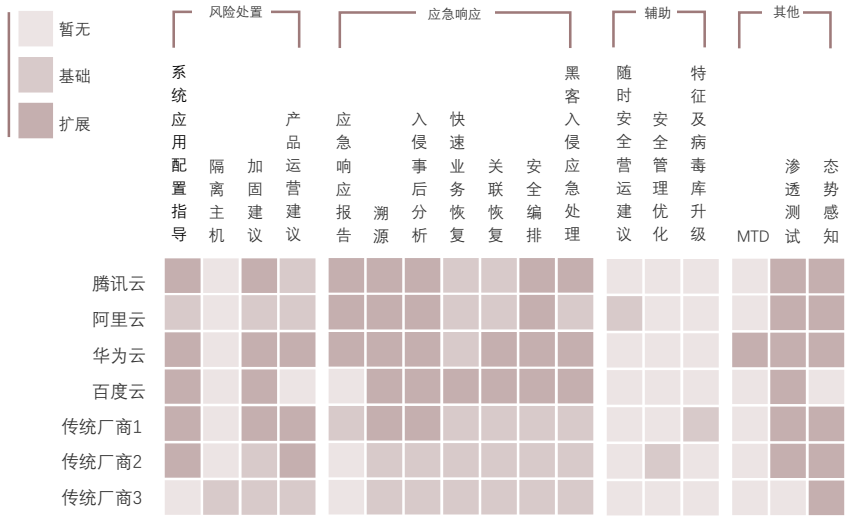
扫描及监控服务模块主要集中于根据企业威胁事件对企业IT资产或云资产的重要度、漏洞（续下页）

中国安全托管服务基础能力——响应处置及辅助

响应处置及辅助模块通过整合安全日志及威胁情报以支持关联分析，实现对现有攻击类型的快速识别、响应、告警、溯源及快速处置，缩减系统恢复周期，降低业务损失

安全托管供应商服务及相关基础能力对比（二）

响应处置及辅助服务模块



（接上页）严重度、网络暴露面等多维度进行综合梳理及实时监控，进而通过风险优先级制定或调整安全防御策略，提升企业网络信息（云）安全策略的全面性、准确性及可持续性。

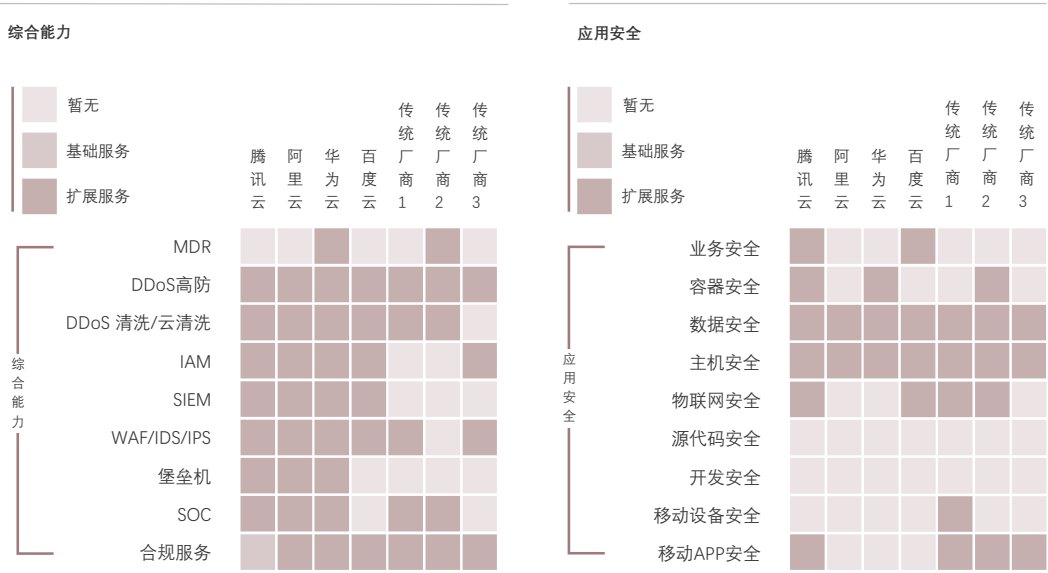
响应处置及辅助服务模块则集中于威胁事件快速识别、关联分析、溯源及响应

响应处置及辅助服务模块则侧重于威胁事件快速响应。安全托管服务供应商主要通过整合相关安全日志及威胁情报以实现对潜在安全风险的关联分析或针对用户异常行为实现用户实体行为分析，以实现对现有攻击类型快速识别、响应、告警、溯源及快速处置，缩减系统恢复周期，进而降低攻击时段内企业业务损失及数据泄露风险。以用户异常行为分析为例，MSSP通过日志方式与网络流量方式等采集方式整合关键数据以提取关键账户、用户、设备、IP等关键信息，运行自动化行为刻画及关联分析，使用孤立森林、SVM、K-Means聚类等机器学习算法进行异常检测，大幅降低预警数量及安全团队分析师工作负载，实现检测周期及准确性的协同提升。此外，该模块负责针对企业配置、风险加固、产品运营等环节提供相关指导及建议，减少企业网络架构中潜在的暴露面及脆弱环节。

中国安全托管服务基础能力——其他能力

不同企业客户在网络架构、企业规模、主营业务等维度存在差异，企业客户受攻击类型、规模及脆弱性异同，安全托管服务边界拓展能力为判断服务商综合能力的重要标准

安全托管供应商服务及相关基础能力对比（三）



■ **扩展服务及相关升级组件可衡量安全服务供应商综合安全能力及潜在安全服务客制化水平**

由于企业客户网络架构、企业规模、主营业务等维度存在差异，个体企业客户受攻击类型、规模及其自身脆弱面均有所不同。同质化的安全托管服务势必难以满足不同企业客户的差异化信息安全需求。因此，以态势感知、渗透测试为代表的定制化服务能力及相关升级组件也同为衡量安全服务供应商定制化服务及综合基础能力的重要标准。

以全球网络安全托管服务龙头企业IBM为例，2016年IBM通过收购Resilient Systems以发展其SOAR产品，并将该产品与QRadar SIEM集成，形成SOAPA解决方案。IBM通过持续收购初创企业以发展其底层安全产品组件布局，扩展服务能力，并根据客户实际需求升级相关组件，进行定制化组合，进而提供更为高效及定制化的网络安全托管服务。IBM整体威胁识别及安全响应效率、安全平台运维效率及团队人机协作效率得以大幅提升。

Chapter 2
下游应用场景

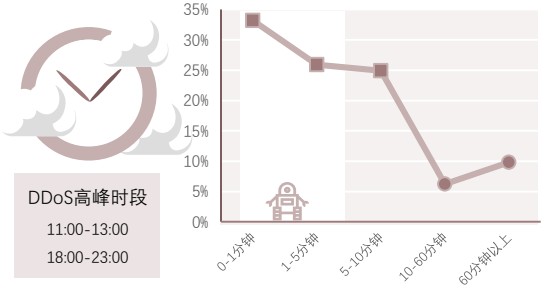
- **中国安全托管服务应用**
  - 行业维度分析

中国安全托管服务应用——垂直行业维度分析

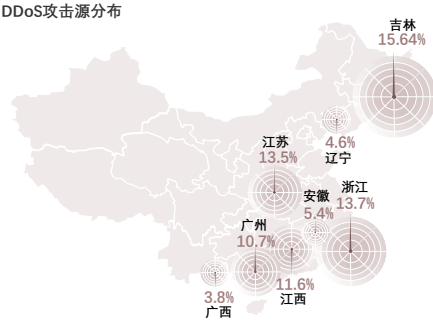
中国游戏行业是网络攻击的重灾区，安全托管服务可针对DDoS攻击提供云清洗及24小时专家服务；2020年疫情推动游戏行业网络安全需求释放，加速安全托管服务应用落地

中国游戏DDoS攻击概况，2019年

DDoS攻击时段与时长



DDoS攻击源分布



游戏行业网络安全市场空间较大，成为中国安全托管服务最快落地行业

2016年后，随中国网络安全行业商业模式逐步从“产品”向“产品+服务” 转型，游戏行业成为中国安全托管服务最快落地行业。从需求侧观察，疫情下中国 “宅经济”的兴起刺激游戏玩家活跃度大幅提升，而针对游戏行业的攻击也随之增加。游戏行业是以DDoS攻击为代表的网络攻击的重灾区，根据沙利文2020年DDoS威胁调研显示，游戏行业攻击次数占比高达79%。从全球游戏公司遭受流量攻击地域分布的角度观察，中国游戏公司受攻击流量的占比高达54%。网络攻击者应用DDoS的攻击方式主要以SSDP反射、NTP反射、SYN Flood Attack小包为主，以实现利用大量互联网僵尸主机在同一时间内大规模消耗游戏系统带宽资源的目的，从而导致服务器系统崩溃。超过80%的DDoS攻击在10分钟以内，主要攻击时段集中于下午19:00至22:00之间，针对游戏业务高峰期进行攻击，导致游戏公司大量损失，游戏生命周期缩短10%-15%。

安全托管服务供应商可提供云端清洗服务，实现针对大规模DDoS攻击抵御

安全托管服务供应商可根据游戏公司需求通过将攻击流量牵引至清洗中心，并将清洗后流量注入目标服务器以实现抵御大规模DDoS攻击的目的。对部分中小游戏企业而言，相较于自建相关抗D系统，由管理安全服务商提供云端交付流量清洗服务，可有效缩减采购设备及安全人员培训等前期安全资金与时间投入，将资源集中于游戏研发及服务器运营，有效发挥其相对优势。同时，安全托管服务可提供专业安全专家技术支持，快速识别攻击类型，并根据不同类型攻击采用相应的防御手段，缩减检测及响应周期，进而缩减中小游戏公司因流量攻击导致的用户流失、数据泄露等风险及损失。

参考来源：《云安全即服务》（周凯），沙利文及头豹研究院编辑整理

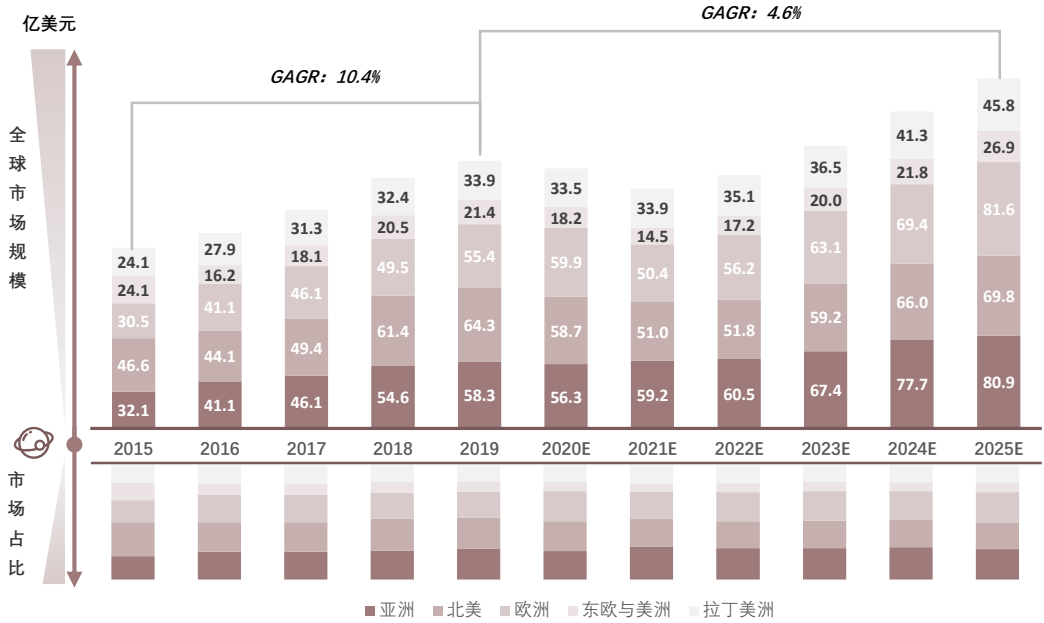
Chapter 3
中外市场对比

- **全球与中国安全托管市场规模**
  - 全球MSS市场规模
  - 中国MSS市场规模
- **安全托管市场差异及发展机遇**
  - 中美市场对比

全球与中国安全托管市场规模——全球MSS市场规模

2020年新冠疫情冲击下，全球商业活动及劳动力流动受阻，进而减缓信息安全服务业务扩张，导致安全托管服务行业增速放缓，行业发展未及预期

全球安全托管服务市场规模，2020-2025年预测



疫情影响全球安全托管服务业务扩张，市场发展未及预期

以安全托管服务为代表的网络信息安全行业受基于信息流规模化群体活跃度的影响较大。2020年新冠疫情冲击下，全球商业活动及劳动力流动受阻，进而减缓信息安全服务业务扩张，导致安全托管服务行业增速放缓。2020年，全球网络安全运维托管服务市场规模预计低于230亿美元，较2019年同比下降5.6%。

海外安全服务供应商整体技术及服务占优，但其内需释放及海外扩张遭遇双瓶颈

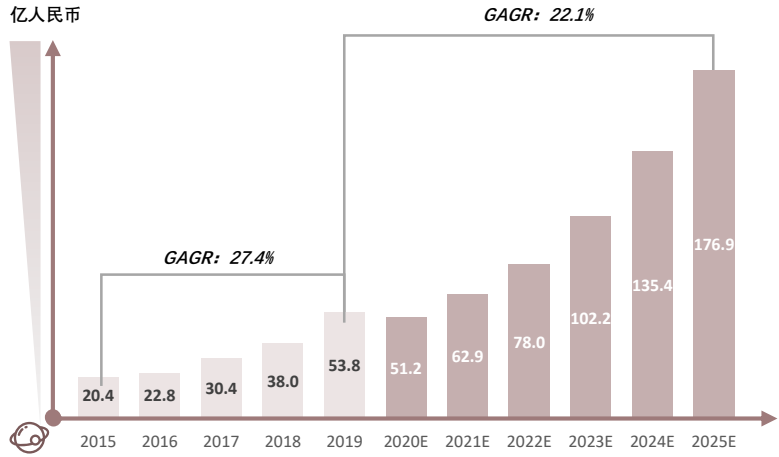
北美与西欧安全托管服务成熟度较高、服务流程及定价标准市场化程度较高，下游需求端市场意愿普及度较高。但受制于疫情，欧美经济收缩严重，导致短期内业务恢复难度较大。同时，由于东西方竞争态势加剧，信息安全敏感度提升。相较于以美国为代表的安全服务领先国家主张以安全标准输出及开放为主导，中国安全托管服务行业暂处于行业追随者地位，偏向于本土安全保护（续下页）

全球与中国安全托管市场规模——中国MSS市场规模

下游中小企业人才技术双缺口带动MSS服务初步实践落地；疫情冲击及地缘争端下，国资入驻及安全标准独立将成为未来MSS行业的本土大型政企市场切入及海外市场扩展的关键

（接上页）及标准独立自主。但传统的安全运维托管行业属于网络安全开放性行业，与中国本土安全方针存在差异，导致海外服务供应商中国市场业务扩展难度增加。

中国安全托管服务市场规模，2020-2025年预测



■ **下游应用需求释放，中小企业率先实现安全托管服务初步实践**

2015年至2019年，伴随云端服务虚拟化及万物互联化，网络开放性端口实现爆发性增长，网络架构脆弱面随之扩大，网络安全需求持续释放。同时，由于网络安全人才供求失衡，导致部分中小企业出现人才及运维安全双缺口，限制企业网络安全持续性战略调整，进一步带动中国安全托管服务实践落地。长期而言，中国安全托管服务市场有望从2020年的51.2亿元上涨至2025年的176.9亿元，年复合增长率高达21.2%。

■ **国际争端加剧，国资背书成为行业发展关键，中国安全托管服务机遇与挑战并存**

2020年，中美地缘紧张局势加剧，冲击全球贸易。同时疫情威胁下，全球经济呈现逆全球化趋势。由于网络安全行业主要依附于业务，经济增速减缓及商业活跃度降低，限制安全业务扩张，整体利空安全托管服务市场。但同时国家层面网络安全标准将进一步升级，国有资本将有望入驻信息安全服务供应商，实现对信息安全领域企业的标准化监督、规模化支持及公信力背书。国资入驻及安全标准独立将成为未来中国安全托管服务行业的本土大型政企市场切入及海外市场扩展的关键。

安全托管市场差异及发展机遇——中美市场对比

中国信息安全产业主张安全标准独立自主，强化中国安全托管服务商本土化优势；同时，一带一路经济数字化战略的推进有望成为中国网络安全服务出海的关键机遇

中美安全托管服务市场差异，2020年

		美国	中国
定义与服务范围	业务范围	涵盖软硬件采购、整合方案、软件升级、后期维护运营的集成化服务	维护运营服务
	售前方案决定权	安全托管服务供应商	客户
	安全标准	标准开放、标准输出	标准保护、独立自主
	市场现况	美国安全托管服务标准化及市场化程度较高、接受度相对较高；此外，美国安全托管服务市场竞争者数量较多，涉及领域较多元、集中度较分散	中国安全托管服务实践暂处于初步阶段，整体产业生态成熟度、客户安全意识、运维服务接受度均存在上升空间；中国安全托管服务行业集中较高，包括以奇安信为代表的安全服务商及以腾讯云为代表的云安全供应商
竞争优劣势	服务优势	服务集成化、定制化、可扩展化程度高、利润空间较大	
	技术优势	行业起步较早，在扫描、清洗及防护等方面占据技术优势，技术自动化及云化程度相对较高	
	市场挑战	客户接受度较高、信任摩擦较小；未来逆全球化趋势限制海外厂商全球性业务扩张	
	市场优势		2020年中国网络安全支出增速为16.8%，领跑全球；未来，随企业安全即服务需求释放，中国安全托管服务市场发展潜力较大
	产业挑战		安全托管服务产业成熟度、客户认可度均存在上升空间。未来国家层面安全力度加强，国资加大安全行业投入，带动安全托管服务商发展力及公信力协同提升
客户群体	企业维度	美国安全托管服务最大安全群体以大型企业客户为主	中国安全托管服务客户为中小型企业，未来国资入驻将推动MSS向中大型政企市场转型
	行业维度	金融服务行业为安全服务市场的主要收入来源，未来有望向医疗行业渗透	中国安全托管服务行业集中于以游戏为代表的泛娱乐行业

中国信息安全体系趋向自主化、独立化，中国厂商本土优势强化：中国信息安全产业主张安全标准独立自主，中外安全托管服务范围及标准体系存在差异，加大海外安全托管服务商在中国市场的扩张难度，为中国本土安全托管供应商提供广大的市场空间。

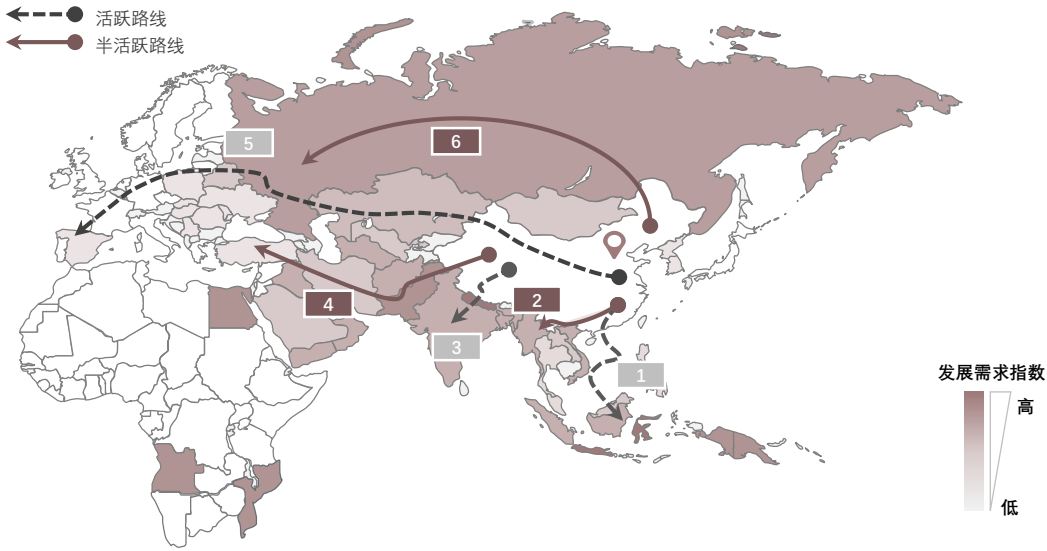
Chapter 4
出海分析

- **中国安全托管出海路径分析**
  - 出海机遇地理分布
  - 出海路径分析
- **中国安全托管出海前沿市场**
  - 前沿市场分析
- **中国安全托管出海潜力市场**
  - 潜力核心市场

中国安全托管出海路径分析——出海机遇地理分布

一带一路沿线国家在关键信息安全基础建设等方面均存在市场上升空间；海外发展中国家信息安全基础环节建设与后期运维需求有望成为国资背景网络安全服务主要发展机遇之一

中国安全托管服务出海“丝绸之路”



- **一带一路倡议沿线国家共建政治互信、经济融合、文化包容的利益共同体**

一带一路是“丝绸之路经济带”及“21世纪海上丝绸之路”的合作倡议，覆盖全球43%的人口及25%的GDP。纵观六大一带一路经济发展走廊，新亚欧大陆桥（5）、中国-中南半岛（1）、中巴经济走廊（3）发展活跃，持续强化政治沟通、设备连通、贸易畅通等目标。

- **安全托管服务出海具备国家安全及出海安全双重意义，深化国际合作，带动中国经济双循环**

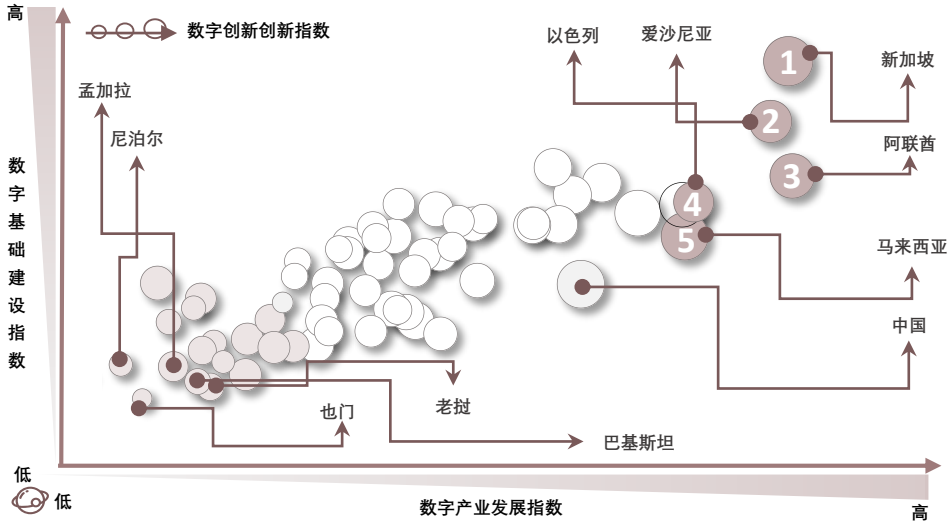
由于网络空间为物理空间的映射，网络安全是国家安全基础。而部分沿线发展中国家在关键信息基础建设、综合安全方案整合及运维管理等方面均存在上升空间，网络安全发展需求较大。该类海外发展中国家信息安全基础环节建设与后期运维需求有望成为国资背景的网络安全服务主要发展机遇。

一带一路倡议下，央企与国企率先实现海外布局。安全托管服务将有效降低网络攻击及数据泄露等风险，保障中国企业海外业务顺利交付及信息安全。同时沿边国家数字化经济能力加强，以中小企业为代表的海外安全运维需求释放，有望进一步扩宽海外安全市场的业务扩张。

中国安全托管出海路径分析——出海路径分析

一带一路国家数字经济发展存在差异，中国安全托管服务出海路径可划分为以新加坡、马来西亚代表的MSS出海前沿市场路径及以老挝为代表的MSS出海潜力市场路径

一带一路沿边国家数字经济发展指数



- **数字经济发展指标是综合衡量一带一路国家网络基础设施、数字化商业需求及人才支撑的指数**

在数字经济发展指数中，数字基础建设指数主要衡量互联网普及度、终端智能化水平等信息基础设施概况；而产业发展指数则侧重于下游应用相关产业的发展水平，如数字政务发展水平及数字商业发展水平。此外，数字创新水平指数则反映一带一路国家的综合人才支撑及人才创新水平。

- **安全托管服务出海前沿市场整体信息规模、商业数字化需求提升，业务扩展潜力较大**

纵观一带一路国家数字经济发展综合水平，新加坡、阿联酋、以色列、马来西亚等海外市场在信息规模化程度及下游应用需求等方面占据绝对优势，整体安全托管服务的海外企业级安全业务扩展潜力较大，未来有望成为传统网络安全供应商及云安全供应商的主要出海落地市场。

- **安全托管服务出海潜力市场信息通讯基础设施发展较为欠缺，整体安全运维需求市场空间庞大**

2013年后，中国持续扶持以巴基斯坦为代表的沿线发展中国家信息网络建设，实现国际友好合作，带动双循环经济发展，同时为中国国资型安全托管服务供应商开辟另一条海外政务级网络安全的可持续增长路径。

中国安全托管出海前沿市场——前沿市场分析（1/2）

新加坡、马来西亚等海外市场在信息规模及下游应用需求等方面占据绝对优势，整体MSS海外企业级安全业务扩展潜力较大，未来有望成为常规型MSSP主要出海实践落地市场

中国安全托管服务出海前沿市场

	新加坡	爱沙尼亚	阿联酋
业务扩张潜力	2019年GDP [CAGR]：3,720亿美元 [4.6%] 互联网人口数（每百人）：82 安全互联网服务器（每百万人）：822.3	2019年GDP [CAGR]：314.7亿美元 [7.8%] 互联网人口数（每百人）：84.2 安全互联网服务器（每百万人）：927.2	2019年GDP [CAGR]：4,211.4亿美元 [4.6%] 互联网人口数（每百人）：90.4 安全互联网服务器（每百万人）：294.4
数字发展潜力	数字产业发展指数：150.3 数字基础建设指数：156.4 数字创新指数：150.4	数字产业发展指数：148.1 数字基础建设指数：140.6 数字创新指数：130.6	数字产业发展指数：150.8 数字基础建设指数：126.4 数字创新指数：136.8
环境友好程度	政治沟通指数：16.9 建设联通指数：16.9 资金融通指数：15.8	政治沟通指数：10.8 建设联通指数：12.0 资金融通指数：10.2	政治沟通指数：12.8 建设联通指数：16.3 资金融通指数：15.4
潜在安全需求	■ 网络篡改：2019年新加坡873个网站遭到篡改，数量同比增长44%。 ■ 恶意软件：2019年CSA在新加坡检测到约530台特殊C&C，相较2018年增长230台。	■ 数据泄露：2019年爱沙尼亚已成为数字化程度最高的国家；99%爱沙尼亚公民使用电子身份证，并可接入超过4,000项数字化服务。由于整体信息流规模化程度较高，网络攻击及数据泄露影响力随之上升。	■ 物联网安全：2020年后阿联酋被评为最具备智慧城市商业潜力的国家之一，但智慧城市物联网设备的大规模应用扩大本地网络攻击面。阿联酋平均每天受到304次攻击。同时，超过42,500个IP摄像机存在GCC网络攻击风险。

中国安全托管出海前沿市场——前沿市场分析（2/2）

马来西亚及新加坡具备营商环境、行业应用、企业需求三大优势，未来有望成为最具前景核心出海市场；短期而言，中国MSS出海目标受众为海外中小企业及中国互联网出海企业

中国安全托管服务出海前沿市场

	以色列	马来西亚
业务扩张潜力	2019年GDP [CAGR]：3,946.5亿美元[6.8%] 互联网人口数（每百人）：71.5 安全互联网服务器（每百万人）：254.3	2019年GDP [CAGR]：3,646.8亿美元[4.7%] 互联网人口数（每百人）：67.5 安全互联网服务器（每百万人）：88.5
数字发展潜力	数字产业发展指数：137.1 数字基础建设指数：118.8 数字创新指数：137.6	数字产业发展指数：137.4 数字基础建设指数：110.5 数字创新指数：145.1
环境友好程度	政治沟通指数：10.9 建设联通指数：16.9 资金融通指数：14.8	政治沟通指数：15.3 建设联通指数：15.1 资金融通指数：16.1
潜在安全需求	■ 安全漏洞：2021年1月，以色列安全公司JSOF披露了7个DNSpooq漏洞，可被应用于DNS缓存投毒、远程执行代码和拒绝服务攻击，影响力辐射本地数百万设备。	■ 恶意攻击：2021年骇客组织“马来西亚匿名者”公开宣称将发动#OpsWakeUp21，重点攻击政府网络和用户线上资产，其影响范围覆盖4,600万本地移动用户。

前沿市场优势分析

■ 纵观出海前沿市场，马来西亚及新加坡有望成为最具前景的海外布局市场；市场优势有三：

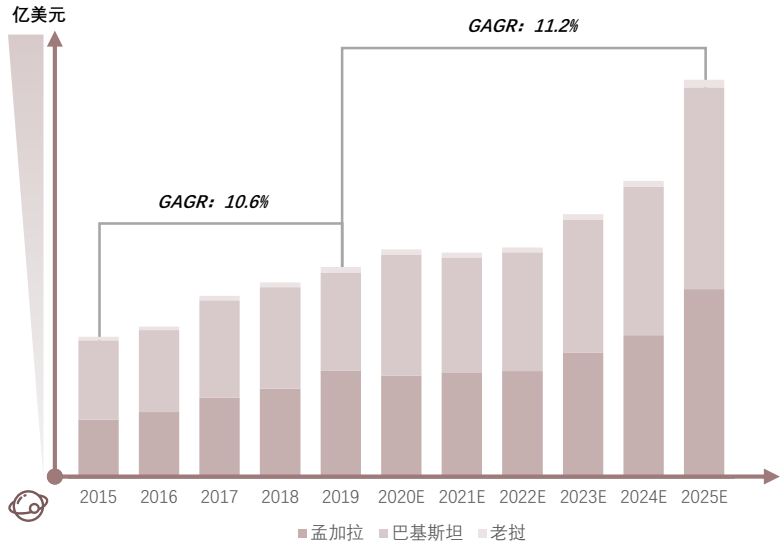
1. **营商环境优势：**相较于北约及中东国家，以新加坡及马来西亚为代表的东南亚国家整体政治局势稳定度、外商开放度、与中国的政治友好度高。同时由于地缘文化与语言相似，中国托管安全服务“本地化”运营及业务扩张成本相对较低。
2. **行业应用优势：**新加坡及马来西亚等东南亚城市整体互联网平均渗透率超过70%。同时亚太地区人口结构相对呈现年轻化特点，线上游戏、线上交友、视频等互联网应用活跃度相对较高，为中国安全托管服务提供海外市场切入点。
3. **企业需求优势：**亚太中小企业普遍缺乏正式且专业网络安全团队。仅有27%的中小企业部署专注于网络安全的正式IT团队，这将限制企业网络安全运维持续性战略，从而引发额外安全风险。

■ **目标客户群体**：由于本地及IBM等海外安全运维服务商进入市场相对较早，针对大型企业安全需求市场竞争难度较高。因此，短期而言，中国托管网络安全服务出海主要市场切入点为海外中小企业及中国互联网出海企业的安全运维需求。

中国安全托管出海潜力市场——核心潜力市场

短期而言，孟加拉等五国重心仍集中于通讯基础设施建设；未来随基础设施完善，互联网信息流规模释放，基础设施等层面安全需求扩大，必将驱动整体网络安全需求增长

孟加拉、巴基斯坦、老挝安全托管服务市场规模，2020-2025年预测



基建需求大于网络安全需求，限制中国安全托管服务短期切入市场与扩张

孟加拉、巴基斯坦及老挝三国在通讯基础技术及设施建设的完善程度均存在上升空间，进而限制整体信息安全需求释放。以老挝为例，2020年老挝地区平均下载网速为4.03Mbps，仅为新加坡地区的1/5，整体信息流规模化程度较为欠缺。此外，当地政府发展仍重点集中于通讯基础设施建设，而对网络安全防护的考量相对较少，导致安全托管服务市场扩张进程较为缓慢。

政府海外基建投资及国际交流带动中国安全托管服务海外市场扩宽

随着孟加拉、巴基斯坦及老挝三国通讯基础设施完善，当地互联网信息流规模释放，网络信息层面、网络运行层面、基础设施层面、核心技术层面及数字货币层面安全关注度将随之上升，进而驱动整体网络安全需求增长。同时，一带一路场景下，国际合作进一步引导中国安全托管服务商与当地需求对接，实现中国安全托管服务出海实践快速落地。

Chapter 4
发展趋势

- 中国安全托管服务技术趋势
  - 无监督学习与ATD
- 中国安全托管服务形态趋势

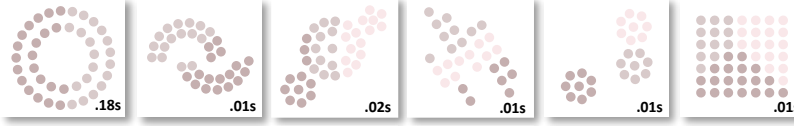
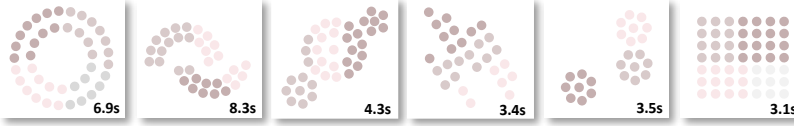
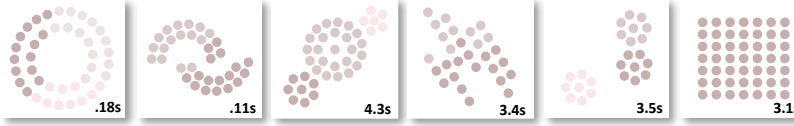
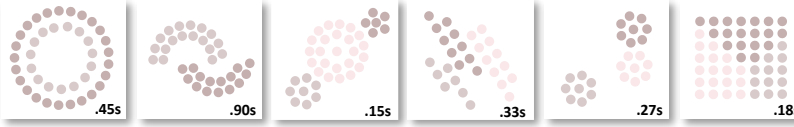
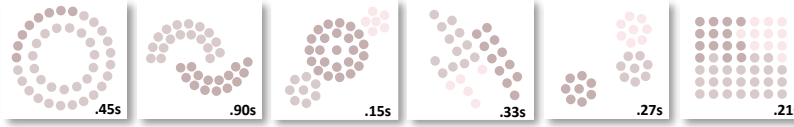
中国安全托管服务技术趋势——无监督学习与ATD

无监督学习通过聚类算法有效解决安全数据膨胀及信息杂乱等数据标注难的问题；在云上及传统MSS应用领域，无监督学习主要应用于ATD系统集成，实现快速及智能威胁识别

■ **无监督学习有效避免数据标注过程，从而提升ATD威胁识别效率**

由于数据膨胀及信息杂乱，网络威胁数据难以显现分类标注，导致系统计算层难以运用标准及准确样本进行机器学习。针对样本数据标注难等问题，无监督学习可摆脱数据标注依赖，通过将数据聚类法以实现无样本标注情景下的自主学习。根据聚类过程差异，无监督学习聚类可分为距离聚类、核密度聚类及层次聚类。其中，距离聚类算法应用最为广泛，主要通过对于距离中心点的持续迭代修正将样本归类于不同的样本簇；其实现关键在于数据事件及事件间距离的界定及初始簇的数量。而核密度及层次聚类则是分别根据初始密度及节点分层实现数据样本聚类。在云上及传统MSS应用领域，无监督学习聚类与ATD（深度威胁识别）系统集成应用，进一步实现快速智能威胁识别。

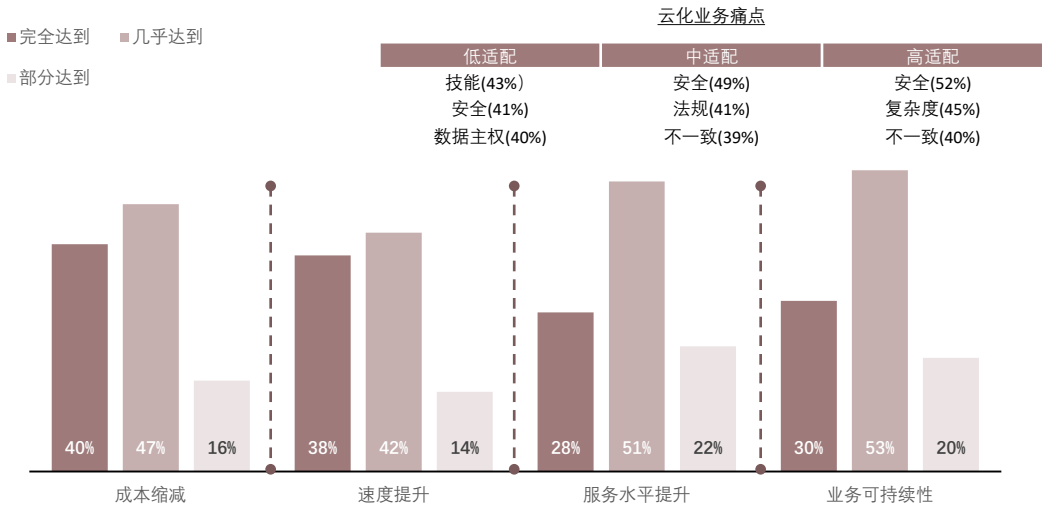
无监督学习聚类算法对比

	聚类算法流程	聚类算法维度对比
K均值聚类		■ 参数：簇数量 ■ 延展性：较大 ■ 应用：通用
AP聚类		■ 参数：减幅 ■ 延展性：不可 ■ 应用：大量簇，规模不均、几何不平坦
均值迁移聚类		■ 参数：样本带宽度 ■ 延展性：不可 ■ 应用：大量簇，规模不均、几何不平坦
谱聚类		■ 参数：簇数量 ■ 延展性：中等 ■ 应用：少量簇，规模不均、几何不平坦
凝聚层次聚类		■ 参数：簇数与阀值 ■ 延展性：较大 ■ 应用：大量簇、可能存在连点限制

中国安全托管服务形态趋势——云端虚拟化趋势

云计算已成为全球经济数字化转型的关键，云安全运维需求逐步释放；同时云化MSS将通过云扫描、云SIEM等方式确保企业客户关键业务资产在多云环境安全状态一致性及无缝性

业务云化优势及云化痛点



云计算已逐步成为全球经济数字化转型的关键，企业安全需求随之“云端虚拟化”

在商业价值方面，云计算在成本缩减，服务水平提升等方面占据绝对优势。根据沙利文及头豹研究院数据显示，受访企业表示 “上云”在成本效益、市场扩张速率等方面达到预期水平。企业未来云端虚拟化有望成为全球趋势。同时由于网络架构日趋复杂，云化企业安全需求随之释放：同时，超过40%的云用户认为安全为最主要云化阻碍。用户侧强需求有望带动安全托管服务向虚拟化交付的方向发展。

云化安全托管服务可基于多住户架构为云客户提供动态云扫描、云防护、云SIEM等安全服务

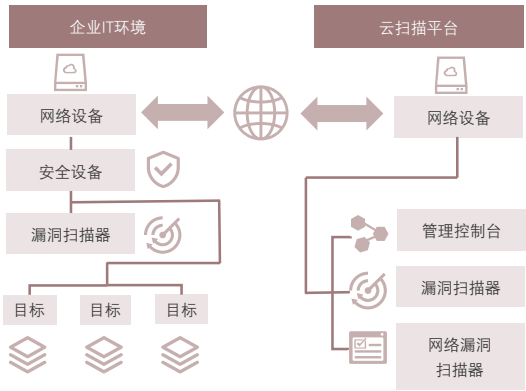
安全托管服务商通过云化安全监管及运维服务实现安全快速响应、数据泄露，确保企业客户关键业务数据资产在多云安全状态一致性及无缝性。相较于传统安全服务，云化安全托管服务在服务弹性、安全服务边际效益、成本节约等方面均占据相对优势。在全球市场中，安全运维即服务、云SIEM即服务相关云化安全托管支付渗透率不到4%。未来随着安全即服务风潮推进，云端部署的安全托管服务将成为主要趋势。从服务环节的维度观察，中国安全托管服务形态趋势可简要划分为（1）云化风险检测；（2）云化安全分析及应急响应。

中国安全托管服务形态趋势——云化风险检测（1/2）

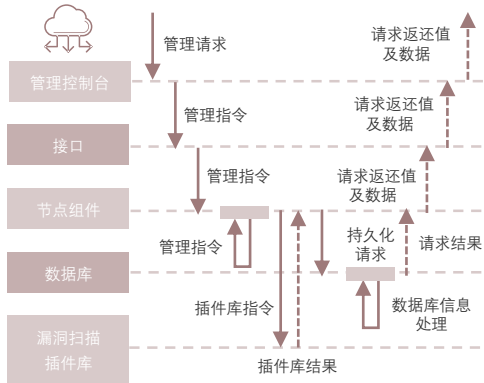
云端漏洞感知及风险检测服务的核心为云扫描，架构由云扫描平台和企业网络环境构成；云扫描平台负责计算、存储等基础架构，对扫描节点进行统一管理，下达扫描管理指令

云化安全：云扫描架构

云端扫描架构



云扫描流程



■ **云端漏洞感知及风险检测服务的核心为云扫描服务**

云端漏洞感知及风险检测服务的核心为云扫描服务；云扫描服务是传统网络安全脆弱性管理的云化服务。不同于传统网络安全扫描，云扫描架构由云扫描平台和企业网络环境两大板块组成。云扫描平台为服务供应商的基础运营平台，主要负责支撑计算、储存、网络等平台底层基础架构，同时提供管理控制台以接收和处理用户请求并对扫描节点组件子模块进行统一管理，从而实现扫描管理指令下达、数据信息处理、结果返还读取等功能。而在企业内部IT环境主要通过漏洞扫描器部署进行企业内部安全漏洞扫描，再将扫描结果返还值返还至管理控制台进行统一整合分析。

■ **云扫描服务主要涵盖企业资产扫描、漏洞扫描、网站扫描、安全配置评估及网络暴露面扫描**

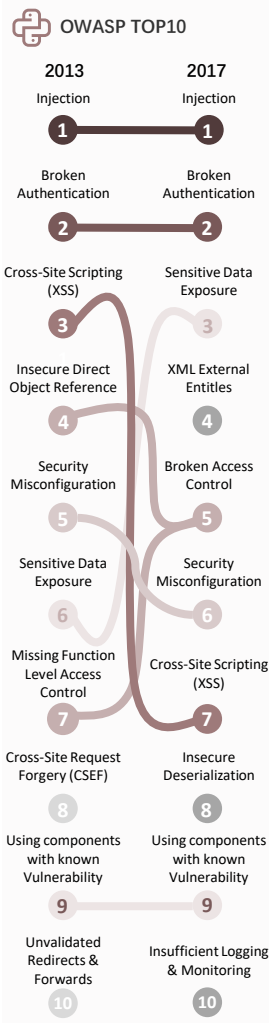
为全面剖析企业资产重要度、漏洞严重度及网络暴露度以形成企业风险优先级划分，云扫描服务主要涵盖企业资产扫描、漏洞扫描、网站扫描、安全配置评估及企业网络暴露面扫描等五项子服务。

- **资产扫描**：云资产扫描与传统IT资产管理相似，主要针对企业IT资产存活、开放端口、服务端口运行等情况进行系统性的主动式网络层扫描及被动式流量监控，同时实现外部攻击路径模拟及内部软硬件资产真实流量梳理。同时，针对于云端虚拟环境，云扫描可通过云开放接口直接获取企业云上资产信息，从而进一步整合信息以形成企业IT资产画像、确定资产重要性分级。（续下页）

参考来源：《云安全即服务》（周凯）、北京邮电大学网络与交换技术国家重点实验室（胡小明、徐鹏），沙利文及头豹研究院编辑整理

中国安全托管服务形态趋势——云化风险检测（2/2）

云扫描服务主要涵盖企业资产扫描、漏洞扫描、网站扫描、安全配置评估及企业网络暴露面，全面梳理企业资产重要度、漏洞严重度及网络暴露度，进而实现风险优先级划分



（接上页）

- **漏洞扫描**：云端安全托管服务及扫描服务供应商通过对企业信息系统、技术及产品中存在的安全缺陷（漏洞）进行识别扫描，同时与CVE、CNNVD、CNVD等安全漏洞库进行匹配以确认漏洞严重程度及对企业潜在威胁影响力。以CVE为例，2018年，各安全及互联网厂商检测漏洞数量超过18,000例，同比增长27%。威胁企业环境的漏洞占比达23%，其中三分之二为高度严重性漏洞（CVE7.0-10.0）。扫描并匹配漏洞库将有效避免未知安全系统缺陷对企业传统网络及云架构的业务运行及数据资产安全可能造成的潜在威胁。
- **网站扫描**：网络扫描运用网络爬虫技术对网站应用资产进行快速遍历性扫描、再根据OWASP TOP10列举的SQL Injection、Broken Authentication、Sensitive Data Exposure等常见网络安全威胁进行集中针对性扫描排查，从而识别企业网络应用业务在编程及逻辑设计中出现的漏洞，进一步获取企业漏洞严重性信息。同时，云扫描服务可通过外部互联网进行网站扫描进一步排查企业网站潜在漏洞暴露情况。
- **互联网暴露面扫描**：根据企业网络架构设计差异，个体企业网络安全的互联网暴露面不同，企业脆弱环节及安全防御范围均存在差异。安全托管服务及扫描服务可通过互联网IP访问网站扫描确认企业外部暴露的安全风险及网站关键数据信息脱敏情况。
- **安全配置评估**：不同于上述对个体资产的扫描，安全配置评估主要针对企业资产基础配置情况进行识别评估，进而形成相关操作系统及技术的安全配置规范以进行相应核查，从而避免因服务器、虚拟机等IT资产配置不当引发的额外安全风险及财务损失。

参考来源：《云安全即服务》（周凯），沙利文及头豹研究院编辑整理

Chapter 5
竞争格局

- **中国安全托管服务竞争格局**
  - 竞争力评价维度
  - 综合竞争力表现

中国安全托管市场竞争——安全托管竞争力评价维度

沙利文设定基础指数、成长指数、服务能力、市场影响力四项评审维度，对中国本土供应商安全托管服务竞争力进行多因素分层次评估

	细分指标	指标要点	指标权重(100%)
基础指数	威胁检测能力	判断供应商安全托管在威胁检测广度、检测速度、准确度等方面的表现	
	事件响应能力	判断供应商安全托管于事前、事中、事后闭环处理安全事件的能力	
	威胁情报能力	衡量供应商安全托管服务融合威胁情报的广度以及情报更新时效性等	
	漏洞验证能力	衡量供应商安全托管对安全漏洞探测、监测的时效性等	
	安全溯源能力	分析供应商安全托管服务对攻击行为进行完整追踪、溯源的能力	

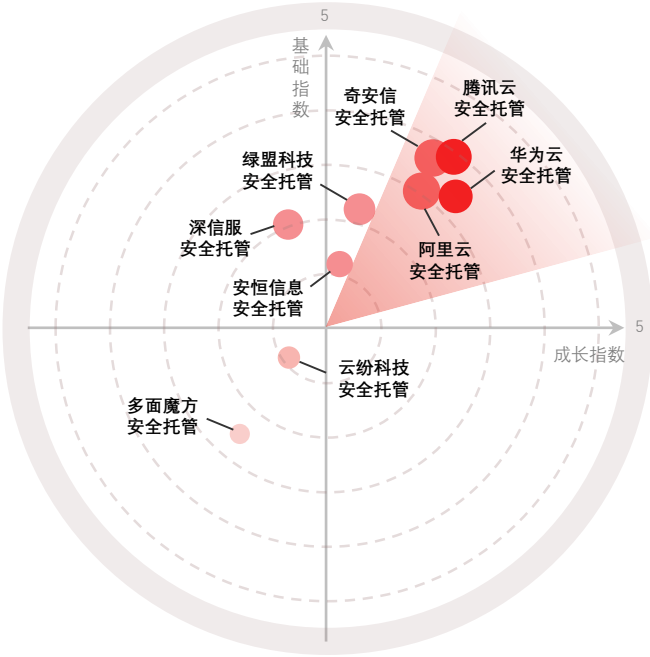
	细分指标	指标要点	指标权重(100%)
成长指数	集成机器学习	判断供应商于安全托管服务后端集成机器学习技术的深度	
	集成SOAR分析	判断供应商于安全托管分析系统集成SOAR工具的广度	
	集成态势感知	分析供应商安全托管服务融合态势感知平台能力的深度	

	细分指标	指标要点	指标权重(100%)
服务能力	适配能力	衡量供应商安全托管服务系统适配不同用户IT架构和业务场景的能力	
	团队配置	判断供应商安全托管服务团队人员构成、人员资质	
	定价策略	衡量供应商安全托管服务定价机制的系统性及灵活性	
	服务多样性	判断供应商安全托管服务支持下游用户定制化需求的范围和能力	

	细分指标	指标要点	指标权重(100%)
市场影响力	用户数	统计供应商安全托管服务在中国境内市场的用户数量	
	市场份额	统计供应商安全托管业务在中国境内的市场份额占比	
	市场广度	衡量供应商安全托管服务在下游行业领域的覆盖广度	

中国安全托管市场竞争——安全托管综合竞争力表现

腾讯云、奇安信、华为云、阿里云入围中国安全托管服务市场领袖梯队，以腾讯云为代表的云厂商领先推动安全托管服务云化、标准化和智能化



领袖梯队

■ 红色扇区供应商入围领袖梯队

领袖扇区圆环按由内向外递增的逻辑对应由低至高的品牌综合评分。综合评分由“基础指数”、“成长指数”、“服务能力”以及“市场影响力”四个维度综合计算得出；

中国安全托管服务市场处于战略转型期，本报告对竞争主体安全托管服务综合竞争力的分析结论仅适用于该阶段市场发展情况。沙利文将持续关注中国及境外安全托管服务市场，追踪品牌动向。

- **纵坐标**代表“ 基础指数”：

衡量竞争主体安全托管服务在基础安全防护方面的竞争力，位置越靠上方，安全托管服务的基础安全能力越突出。

- **横坐标**代表“成长指数”：

衡量竞争主体在安全托管服务中有机融合新技术、新架构的广度、深度，位置越靠右侧，安全托管服务的成长力越显著。

- **色深**代表“服务能力”：

衡量竞争主体安全托管服务在适应性、多样性、性价比等细分维度的表现，色深越深，代表厂商安全托管的服务能力越优秀。

- **气泡大小**代表“市场影响力”：

衡量竞争主体安全托管服务在市场份额、用户渗透力等细分维度的竞争力，气泡越大，代表厂商安全托管服务市场影响力越强。

中国安全托管市场竞争——领袖梯队：腾讯云

依托云原生架构、SOAR自动化工具以及庞大的安全情报体系，腾讯云加速推进安全托管服务标准化、结构化进程，并通过灵活的服务方案提供更加精准的MSS安全运维策略

主导MSS标准化进程：提升安全托管解决方案的系统性、结构性

腾讯云安全主导更趋流程化的安全托管服务策略，持续提升托管安全运维界面灵活性和友好度，依托标准化工具助力政企用户应对更加活跃、复杂、呈指数级增长的外部威胁，降低用户资产安全运维的复杂性。对于供应商而言，托管安全服务标准化的推进有助于优化人员配置，提高人员配置率，降低托管服务成本。对于下游用户而言，全链路、流程化的业务资产安全托管，有助于提升安全团队快速应对新型变种网络攻击的能力，更好地应对未来3至5年数字化转型过程中可能遇到的系统性和非系统性风险，并评估未来更长时期内适合企业自身业务模式的安全运维策略。

云原生自动化分析：灵活方案助力用户应对云计算场景安全新挑战

腾讯云上安全托管服务集成安全运营中心数据整合及分析能力，基于云上标准化工具为用户本地安全管理赋能，并通过服务方案的灵活配置，延长安全模型生命周期，强化安全模型复用力。依托云原生架构，腾讯云MSS团队为用户提供精准的安全运维策略及主动防御能力，进而支持中小企业用户在业务信息化转型过程中实现可持续增长。

安全情报、安全防护技术加持：7大安全实验室为MSS服务夯实基础

腾讯安全联合实验室持续推进安全防护技术的进步，为安全托管服务的推进奠定切实基础。云鼎实验室持续更新云端APP安全方案和虚拟化安全技术，加速云上安全托管服务的应用和普及，进一步提升中小企业用户应对安全风险事件的快速响应能力，进而推动中国云安全托管服务市场扩容。

整合SOAR工具：推进安全监控系统自动化运转效力

腾讯云推出自研SOAR平台，通过集成云原生安全数据，构建安全编排自动化平台、安全事件响应平台以及威胁情报平台。SOAR平台支持多场景安全剧本以及多安全设备联动，有助于推动MSS工作流程的自动化、标准化，提升云MSS服务人机协同效率。

基于基础安全研究能力，深度融合云原生架构及SOAR自动化能力，打造MSS服务闭环

政企用户业务资产上云
安全暴露面年增长率>200%
腾讯主导公有云安全运营服务

腾讯云MSS "IPDRR" 模型

- 应急响应值守
- 风险检测
- 安全监控
- 安全风险评估
- 漏洞感知与风险监测
- 风险处置

自研SOAR平台	云原生安全数据	基础安全研究能力
SOAR工具、流程自研	构建多元云原生工具	7大安全实验室
打造自动化工作流系统	漏洞扫描系统秒级响应	持续挖掘高危漏洞
上线安全编排剧本>10	自研云合规镜像系统	虚拟化安全技术持续升级

MSS服务闭环

方法论

- 头豹研究院布局中国市场，深入研究10大行业，54个垂直行业的市场变化，已经积累了近50万行业研究样本，完成近10,000多个独立的研究咨询项目。

- 研究院依托中国活跃的经济环境，从安全即服务、SOAR、EDR等领域着手，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。

- 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。

- 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。

- 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明

- 本报告著作权归头豹所有，未经书面许可，任何机构或个人不得以任何形式翻版、复刻、发表或引用。若征得头豹同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“头豹研究院”，且不得对本报告进行任何有悖原意的引用、删节或修改。

- 本报告分析师具有专业研究能力，保证报告数据均来自合法合规渠道，观点产出及数据分析基于分析师对行业的客观理解，本报告不受任何第三方授意或影响。

- 本报告所涉及的观点或信息仅供参考，不构成任何投资建议。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。在法律许可的情况下，头豹可能会为报告中提及的企业提供或争取提供投融资或咨询等相关服务。本报告所指的公司或投资标的的价值、价格及投资收入可升可跌。

- 本报告的部分信息来源于公开资料，头豹对该等信息的准确性、完整性或可靠性不做任何保证。本文所载的资料、意见及推测仅反映头豹于发布本报告当日的判断，过往报告中的描述不应作为日后的表现依据。在不同时期，头豹可发出与本文所载资料、意见及推测不一致的报告和文章。头豹不保证本报告所含信息保持在最新状态。同时，头豹对本报告所含信息可在不发出通知的情形下做出修改，读者应当自行关注相应的更新或修改。任何机构或个人应对其利用本报告的数据、分析、研究、部分或者全部内容所进行的一切活动负责并承担该等活动所导致的任何损失或伤害。

www.leadleo.com

https://space.bilibili.com/647223552

https://weibo.com/u/7303360042