FROST & SULLIVAN
沙利文

头豹
LeadLeo

2022年中国
云主机安全市场报告

重点关注：自适应安全、云原生安全、纵深防御等

2022年12月

头豹研究院
弗若斯特沙利文咨询（中国）

报告说明

沙利文联合头豹研究院谨此发布中国网络安全系列报告之《2022年中国云主机安全市场报告》年度报告。本报告旨在分析在中国云工作负载安全市场的现状、应用前景、技术动向及发展趋势，并判断云主机安全市场竞争态势，反映该细分市场领袖梯队厂商的差异化竞争优势。

沙利文联合头豹研究院对云主机安全进行了下游用户体验调查。受访者来自金融、国央企、政务、电信、医疗、教育等不同行业，所在公司规模不一，细分领域有别。

本市场报告提供的云主机安全发展趋势分析亦反映出云主机安全行业整体的动向。报告最终对市场排名、领袖梯队的判断仅适用于本年度中国云主机安全市场发展周期。

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。

报告提供的任何内容（包括但不限于数据、文字、图表、图像等）均系弗若斯特沙利文及头豹研究院独有的高度机密性文件（在报告中另行标明出处者除外）。未经弗若斯特沙利文及头豹研究院事先书面许可，任何人不得以任何方式擅自复制、再造、传播、出版、引用、改编、汇编本报告内容，若有违反上述约定的行为发生，弗若斯特沙利文及头豹研究院保留采取法律措施、追究相关人员责任的权利。弗若斯特沙利文及头豹研究院开展的所有商业活动均使用“弗若斯特沙利文”、“沙利文”、“头豹研究院”或“头豹”的商号、商标，弗若斯特沙利文及头豹研究院无任何前述名称之外的其他分支机构，也未授权或聘用其他任何第三方代表弗若斯特沙利文或头豹研究院开展商业活动。

头豹 LeadLeo

FROST & SULLIVAN 沙利文

研究框架

图表目录

章节一　市场发展背景

1.1宏观建设：云原生安全发展

1.2微观协同：CWPP+CSPM+CASB

1.3环境延伸：从传统主机安全到容器安全

- 鉴于中国市场在安全合规、市场习惯等方面存在的相对于境外市场的差异化特征，安全服务商在引进更为前瞻的技术策略时，宜在可用性和适用性之间进行权衡。

- 从应用距离的角度而言，CASB更加靠近生产端，CWPP则更加靠近IT基础设施管理端。CASB的使用助力企业对云服务在业务中的渗透范围有了全域认知， CSPM在云负载全生命周期的应用过程中适应性不断增强，CWPP针对混合云架构下工作负载提供可视化的管控。

1.1 宏观建设：云原生安全发展

❑ **Agent全方位采集云端资产，应对多变的虚拟环境威胁。**

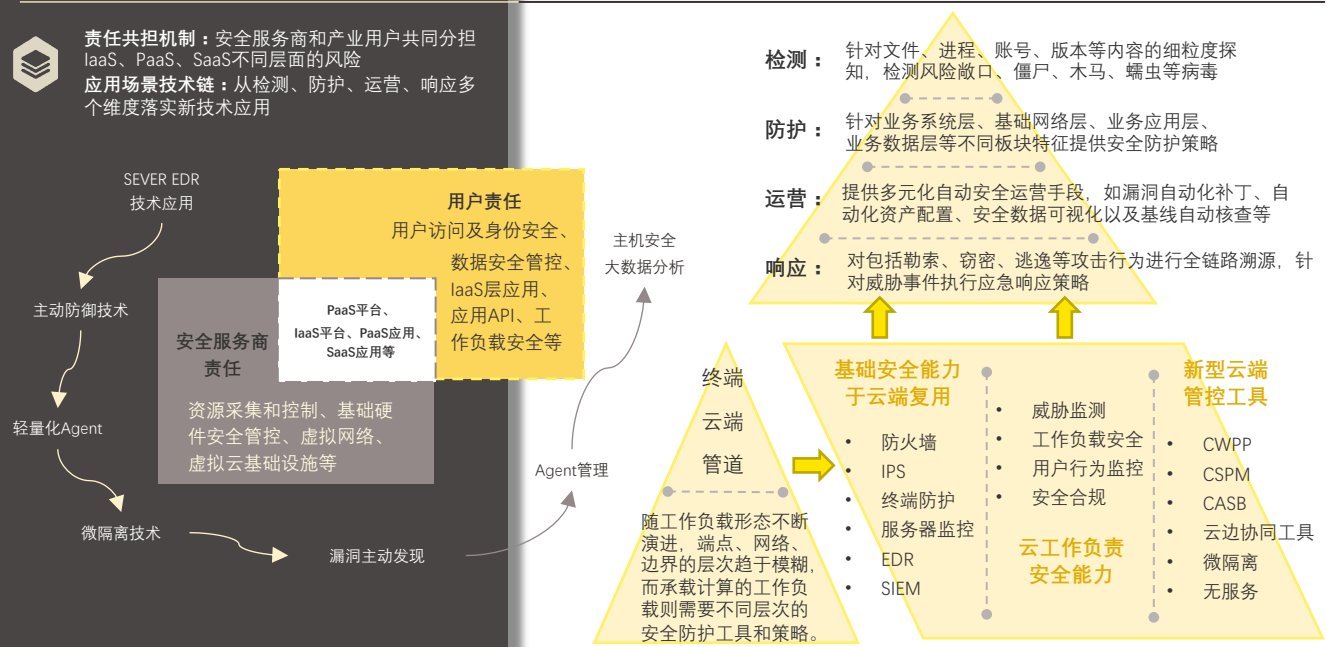
截至当前，中国云计算产业依旧保持较高速增长，预计在未来5年内，90%以上的企业将实现部分业务或关键性业务整体上云。在中国市场环境下，公有云环境可信度相对境外云环境仍存在差距。多数用户偏好“混合云”解决方案，包括传统设备主机、核心私有云、非核心资产公有云以及容器等承载环境。混合云部署方案下，安全防护相关的资产归属和控制机制对安全服务商和用户而言，存在更多合作的机遇和责任共担的挑战。

鉴于中国市场在安全合规、市场习惯等方面存在地域性特征，安全服务商在引进更为前瞻的技术策略时，宜在可用性和适用性之间进行权衡。云原生安全机制的引入，给予中国云安全市场更多的选择，云原生环境的安全事件存在于系统和组件之间，云工作负载安全类产品在对风险进行发掘和重构后，持续设计新的安全功能，最终实现安全机制与云原生系统的全面融合，确保用户安全访问使用云系统和云应用。

❑ **云原生安全环境下的市场机会：**

- **持续交付场景下的实时安全：**企业云上业务更新频率或达每日上百次、上千次，持续开发部署工具链各个环节相关安全检测、监控、防护手段更趋精细化和个性化。
- **广域云工作负载安全防护：**云工作负载环境形态更趋丰富，边界模糊性强，资产暴露面从静态文件至动态中间件皆面临广域的威胁形态，威胁探知能力和应急策略更待精进。

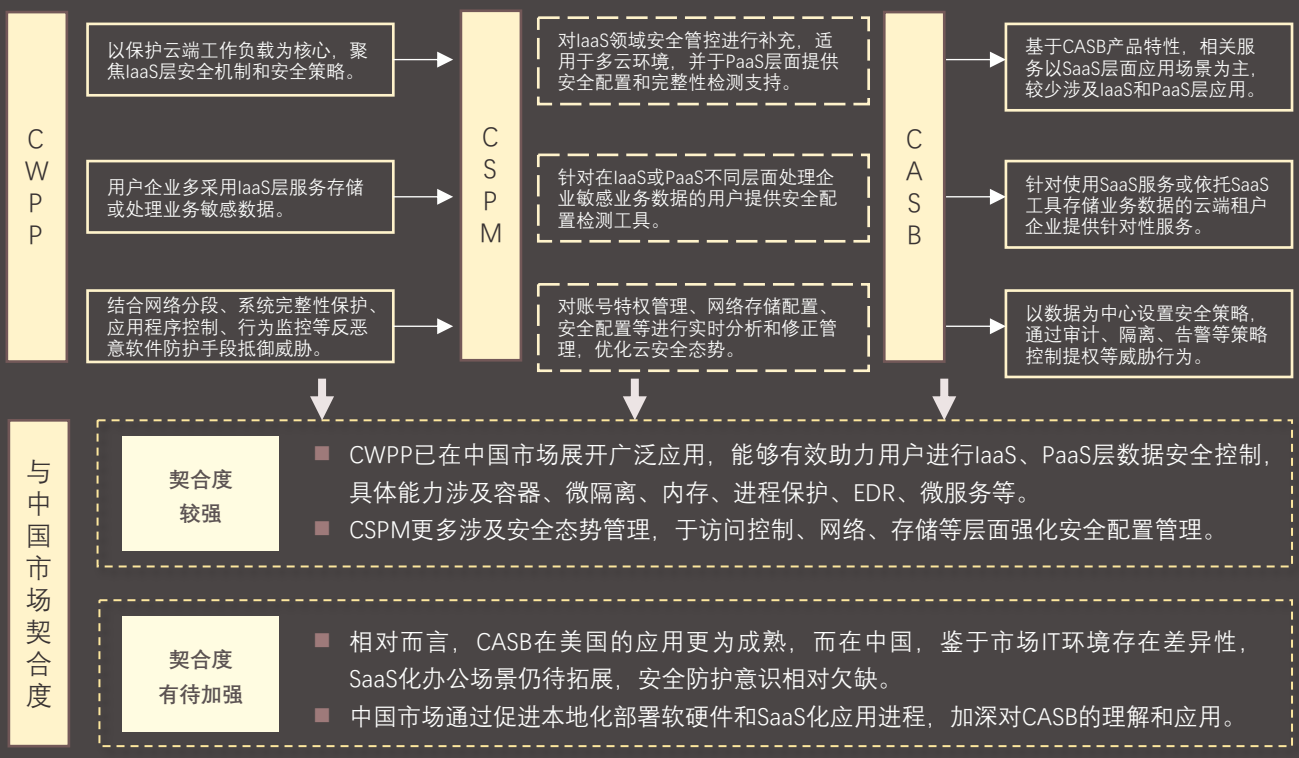
图1：不同部署环境下主机安全责任机制及云上相关服务和组件



1.2 微观协同：CWPP+CSPM+CASB

- CASB (Cloud Access Security Broker) 云访问安全代理，是置于云服务消费者和和提供商之间的安全策略，其覆盖面包括了SaaS、PaaS和IaaS，主要提供针对于SaaS的安全控制。CASB主要具备以下功能：深度可视化、数据安全性、合规性、威胁防护。
- CSPM (Cloud Security Posture Management)云安全态势管理，可同时适用于PaaS和IaaS，主要对基础设施安全配置进行分析管理，也可以强化和检查控制面的安全和正确配置。其安全策略包括管理工作负载、合规评估、保障API完整和运营监控等。若发现不合规配置，CSPM将对其进行修正，并持续改进和适应云安全态势。
- CWPP（Cloud Workload Protection Platform）云工作负载安全防护平台，主要聚焦于IaaS相关的工作负载安全，对云上工作负载提供全方位和多个维度的保护能力。其主要保护范围是IaaS层，可以横跨物理机、公有云、私有云等多种数据中心环境，部署方式因而更加灵活，防护面更广。

图2：CWPP+CSPM+CASB防护策略协同



1.3 环境延伸：从传统主机安全到容器安全

❑ **主机安全系产品核心模块及应用环境变化**：

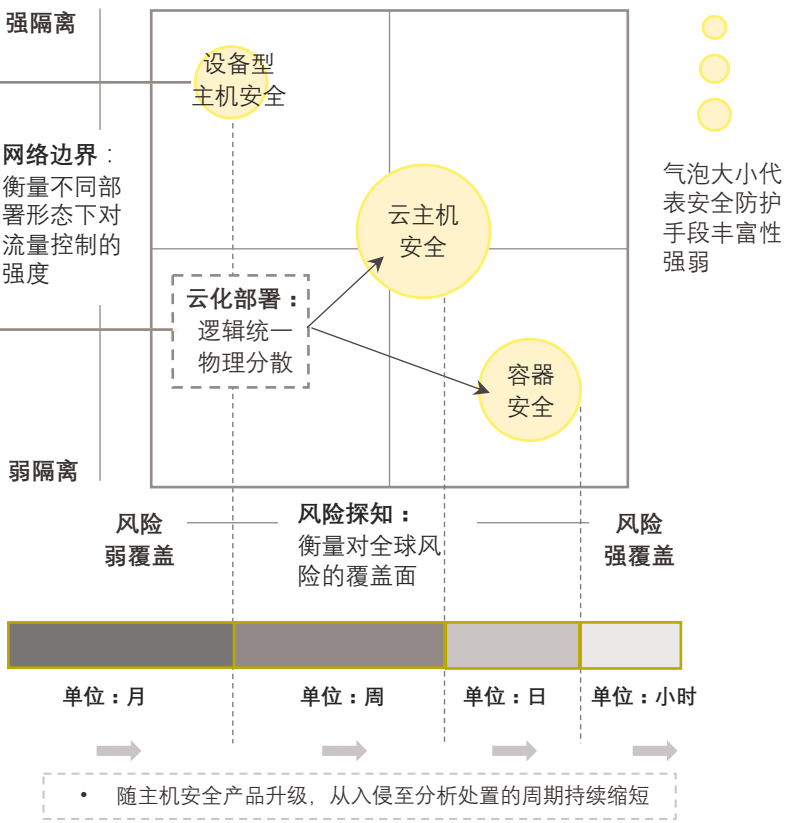
- 基础类主机安全产品聚焦于检测、探知、盘点、合规四个方面。技术叠加效用下，产品模块拓宽至蜜罐、内存码检测、病毒查杀等方面，而随用户侧业务上云、统一安全管理方案建设和产品聚合效用提升，主机安全能力更加收敛于四个核心模块，并在运行环境层面渗透云原生、供应链，头部服务商融合威胁情报系统优化主机产品的检测效率。

❑ **主机安全系产品技术理念迭代：**

- **病毒查杀机制应用：**风险查询和处置多以静态样本为依据，通过在计算机文件和病毒特征码之间进行比对确认风险，存在更新不及时、样本质量参差不齐的缺陷。
- **白名单机制应用：**相对病毒查杀在进程消耗、内存占用等方面可能对业务造成的影响，白名单机制的创建有利于防守加固和前置，降低木马程序对系统的危害。
- **纵深防御机制应用：**利用虚拟化、微隔离、无服务等云原生技术，应对多云和跨云环境下的复杂攻击态势，纵深防御系统与完整性验证、EDR、HIPS等多层次防御策略融合。

图3：主机系安全防护产品特征差异矩阵

- **传统主机安全：**以病毒查杀为主，多为静态查验能力，攻防性质不足，不具备实时检测能力。
- **云负载环境主机安全：**解决方案持续优化，完整覆盖攻击链，支持实时检测和自动分析溯源。



章节二　技术发展动向

2.1中国主流服务商年度发展计划落实现状

2.2中国云主机安全功能模块要点及发展动向

2.3境外主流服务商产品重点能力和竞争优势

- 境外服务商在整体技术栈层面具备较为显著的创新力，在特定漏洞研究以及技术栈升级等方面始终处于领先的地位。境内服务商逐渐通过原厂研究、独立实验室孵化等方式加快技术栈布局。

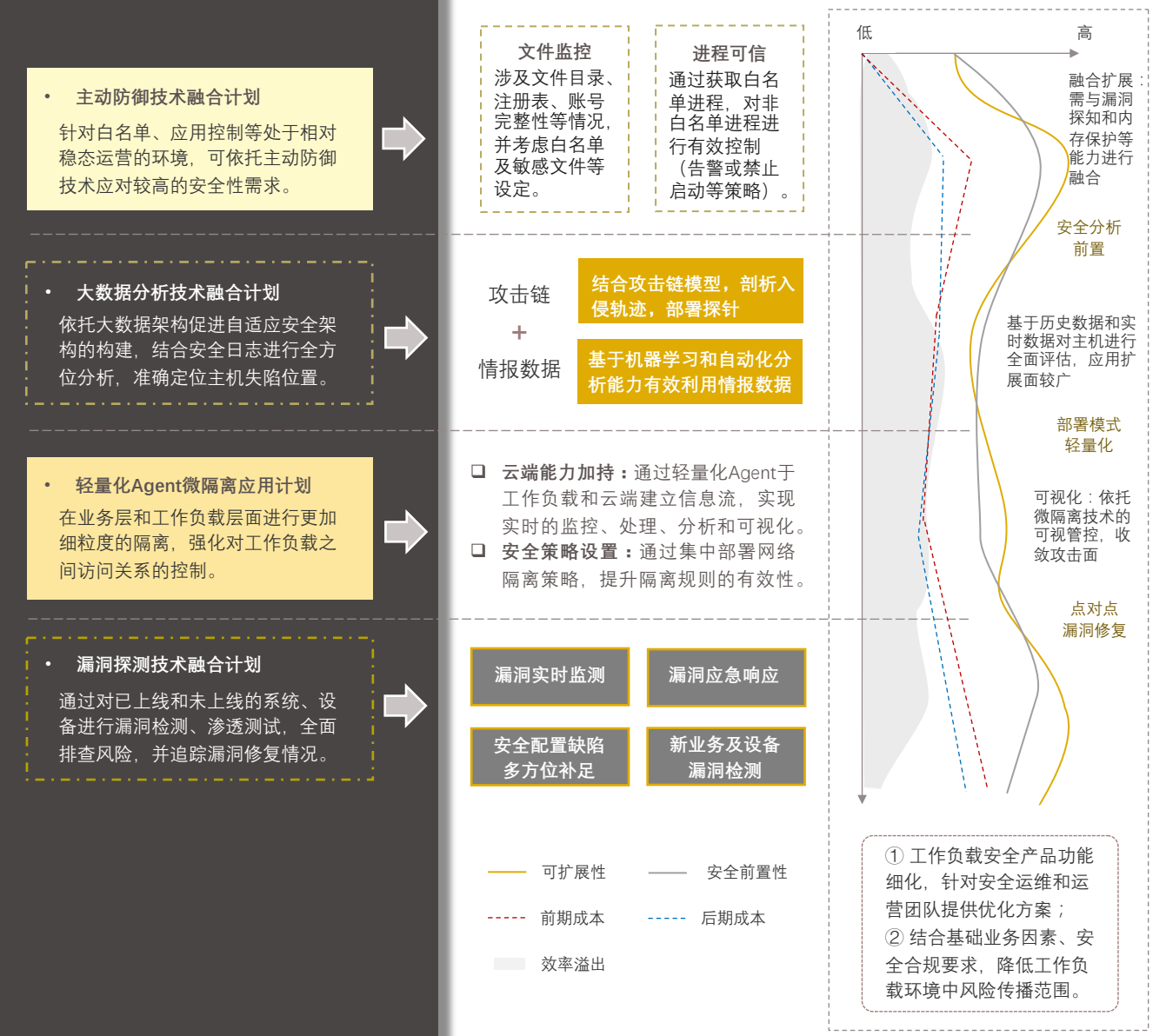
- 尽管在云原生技术方面，境内服务商多以贴合、跟进境外主流技术为主，但通过对境外核心技术进行分解或根据自有产线进行延伸，境内服务商更能根据境内安全环境、业务环境构建服务模式。

2.1 中国主流服务商年度发展计划落实现状

❑ **安全服务商能力进阶：安全分析工具和安全管控工具对用户业务场景适用性增强。**

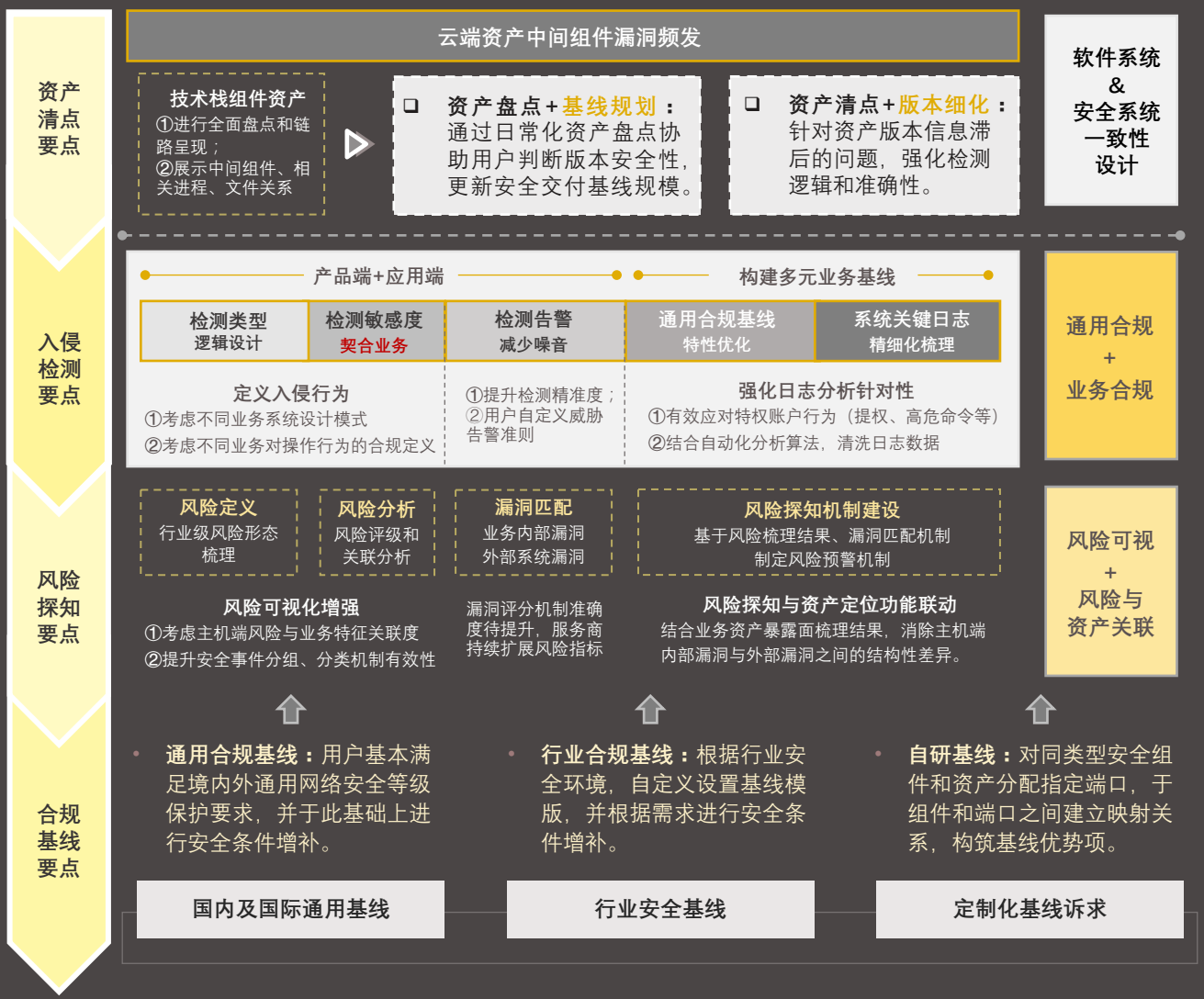
安全服务商于2022年度持续优化云主机安全功能点，提供更加丰富的工作负载安全闭环管理方案，针对挖矿场景、APT攻击场景、勒索场景、窃密木马、常规木马、重保/护网场景等提供更具针对性的防护方案，如收敛资产暴露面、漏洞发现、威胁情报探知、勒索治理、虚拟化补丁等。安全服务商助力用户依托大数据分析平台、机器学习分析引擎、集中部署微隔离策略、主动防御技术等，提升工作负载环境整体安全管控效率，解决传统运维管控方案中存在的难题，扩大自适应架构应用面，并强化主机安全产品与EDR、SOC、SIEM等防护体系的融合。

图4：云主机安全能力发展计划及落实情况



2.2 中国云主机安全功能模块要点及发展动向

图5：云主机安全功能应用现状及诉求要点



▪ 资产清点要点及用户进阶诉求

❑ **功能特征：助力用户提升漏洞应急响应效率及业务影响分析能力**

相对传统物理服务器环境下的业务而言，云端业务所面临的安全态势更加复杂，云端资产中间组件存在漏洞频发的特征。

在此背景下，云端资产盘点更需要针对漏洞影响面规划响应和分析方案。云业务环境所需要的资产清点功能，更需要对技术栈组件进行全面的盘点和进一步的链路呈现。用户诉求要点在于通过全面盘点和展示中间组件及相关进程和文件的连接关系，在漏洞发生时对相关资产进行快速定位、快速梳理。并且通过Agent充分展现资产所遭受风险的严重性和范围。并在此基础上，支持用户对漏洞作出更有效的快速响应。

此外，日常化资产盘点流程能够协助用户规划基线，通过清点的功能，判断应用版本的安全性，进而更新安全交付基线模式。

- **用户进阶诉求：云产业链安全逻辑协同，资产清点细化至版本层面。**

当前，多数服务商支持的资产清点模块在检测逻辑方面，多以进程或目录为对象，存在版本判断准确性不足的痛点，存在版本信息滞后的问题，对用户资产清点结果造成干扰。此外，云端资产清点涉及开源性质文件，对版本盘点准确性的提升需要供应链上游服务商对应用目录进行更加标准化的处理。未来安全服务商或可通过与软件供应链上游参与者提升协同性和设计趋向等方式，提升云环境整体安全系统设计的一致性，进而助力下游用户在资产面和攻击面之间实现更加精准的映射分析，提升漏洞与资产类型之间的关联度。

▪ 入侵检测

- **入侵检测产品端与应用端：用户业务系统对入侵行为定义存在差异**

在入侵检测板块，服务商基本能够满足用户在检测类型、检测敏感度、检测告警方面的需求，入侵检测功能的应用痛点更多缘于不同业务系统设计模式对操作行为合规定义的差异性。

目前，应用端风险探知能力未能有效应对的入侵事件主要存在于特权账户使用行为(包括账户提权、高危命令执行等）。

- **用户进阶诉求：强化日志分析针对性，构建多元业务基线**

安全服务商在对入侵行为定义细化的可行性方面能力有限，此外，造成入侵检测准确性偏差的因素更在于用户业务系统设计结构对风险行为定义的差异性。在部分应用场景下，业务系统常见的提权行为是基于业务后台（如脚本、工具、执行过程）正常实际要求而进行的，但在主机安全防护层面，针对该类偶发性正常提权行为进行规则定义和自动化剥离的可行性较低。

基于应用端特征对入侵检测精准度提升的限制，安全服务商可将注意力集中在优化通用合规行为定义层面，可依托自动化分析算法，结合不同行业业务特征对系统关键日志进行梳理，并通过对长期积累的日志数据进行清洗，形成基线和针对性告警机制。

▪ 风险探知

❑ **用户诉求：风险展示界面优化+风险探知与资产定位联动性强化**

风险探知板块的能力更多体现在对风险的定义、风险漏洞评分和关联、风险分析等方面。主机基础设施是企业建立在业务内部的运行基础，主机风险探测的方式与边界防火墙通过扫描探知风险的方式有较大区别。

主机端所面临的风险类型与业务特征相关度较高，需根据业务资产暴露面梳理和判断主机所遭遇的漏洞与何类漏洞相匹配。部分服务商提供漏洞评分机制，但业务内部漏洞和外部系统漏洞之间存在结构性差异性，故而评分机制缺乏准确性。相对而言，公有云安全服务商在主机漏洞与外部漏洞匹配方面具备优势，可结合公有云上大部分租户对漏洞的判断和修补动作，为更多用户提供决策依据或风险指标。而在私有云环境下，服务商普遍根据用户内部风险面构建风险探知机制，对漏洞进行相应的匹配和分析，在风险展示能力方面略弱于公有云安全服务商。

此外，服务商需持续提升云主机端风险探知和资产清点功能的联动性，通过对资产更加精细化和准确的盘点，对风险和漏洞进行更强的关联，提升安全事件分组、分类机制的有效性。

▪ 合规基线

❑ **功能特征：基于通用性合规指标进行业务安全条件增补**

当前在合规基线模块，安全服务商基本能够助力用户满足国家网络安全等级保护以及CIS考核指标等要求，部分服务商协助用户在通用性标准基础上进行安全条件增补，根据所在行业安全环境自定义设置基线模板，并随自研基线应用的扩展，提升用户内部安全管理策略有效性。

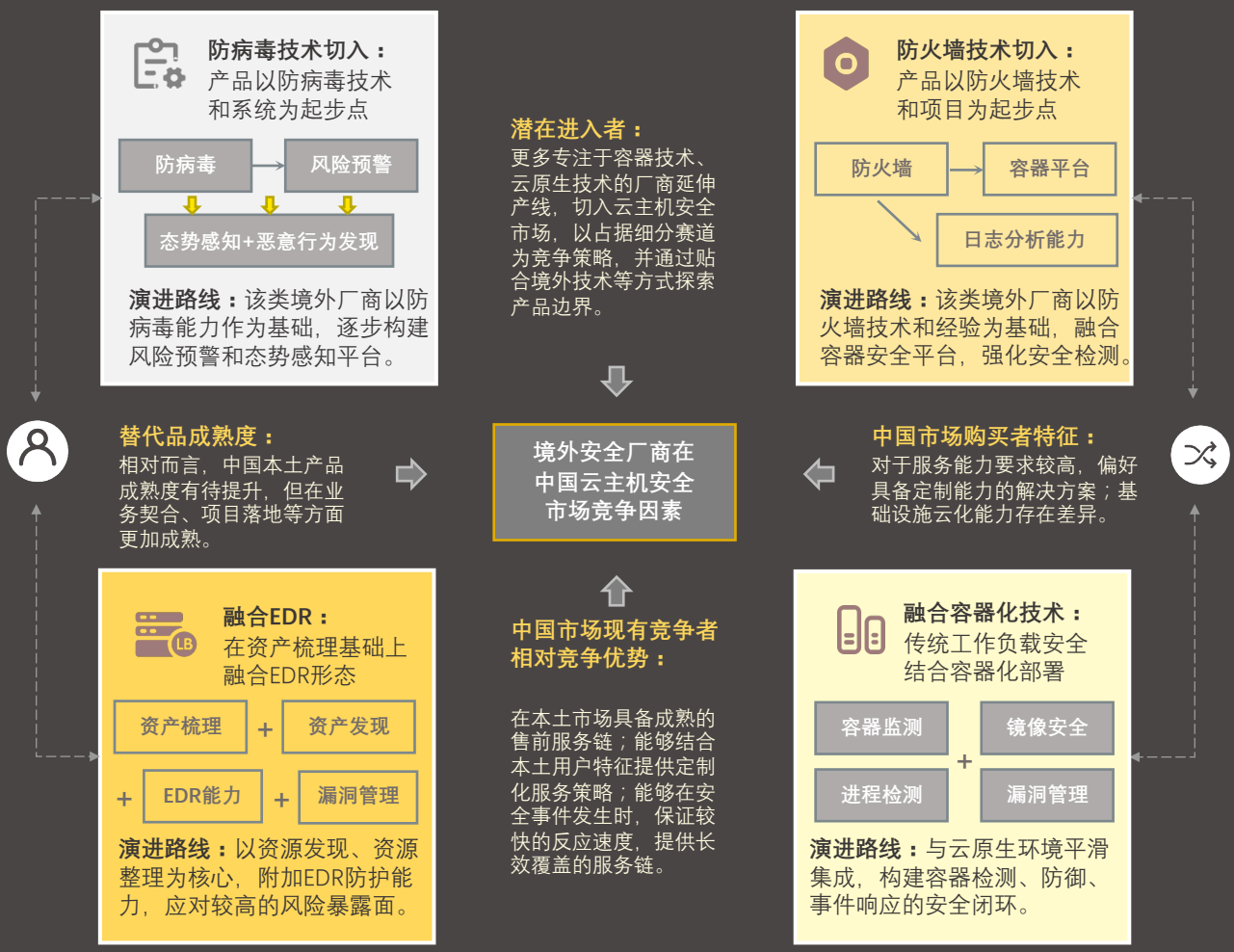
❑ **用户进阶诉求：推进自研基线，提升同类资产与指定端口归类统一性**

安全服务商尚未对组件和端口进行关联性归类处置，不同的安全产品组件分布在不同端口运行，对用户而言，新安全组件增量交付时或面临较高的适应成本和运维成本。

对安全运营能力较为成熟的用户而言，对同类型安全组件和资产分配指定端口的归类方式有助于降低运维成本。通过在组件和端口之间建立一一映射的关系，用户能够更加清晰地盘点资产、定位资产，实现合规基线检验有效性的提升。然而，当前自研基线理念对多数安全服务商而言，在设计逻辑层面存在较大差异性。但远期愿而言，自研基线生态产品的构建或成为安全服务商的优势项。

2.3 境外主流服务商产品重点能力和竞争优势

图6：境外主流服务商云主机安全产品重点能力及在中国市场竞争态势



TREND MICRO

- 价格灵活度待提升
- 部署难易度待改善

- Trend Micro：从防病毒技术栈出发，逐步建立风险预警机制、EDR等与态势感知及恶意行为检测关联度较高的能力。趋势科技产品线渗透端点安全、网络安全、云工作负载安全等广域业务环境，产品之间在底层引擎和上层应用等方面协同整合，作为物理资产虚拟化实践的主导者之一，未来趋势科技在物联网安全、容器安全等领域持续发挥实践引领作用。

- 后期维护服务略弱
- 同行使用者友好度提升

❑ **Palo Alto：**从防火墙业务起步，通过并购Twistlock容器安全平台，逐渐形成云原生安全服务能力。Paloalto构建一整套云原生环境安全策略知识库，通过订阅模式为用户提供体系完善、检索灵活的日志分析能力，并针对容器内应用程序活动、网络活动等，在事前提供有效的安全环境检测策略，是较早覆盖容器全生命周期安全管理的服务商之一。

- 第三方兼容待提升
- 微隔离策略应用需拓展

❑ **Aqua：**在全球范围内引领DevSecOps理念的落地，在产品能力构建方面强化流水线交付模式。着重对容器镜像库内部资源在持续集成和持续交付过程中涉及的安全指标进行有效管理。对于镜像篡改特定进程、木马程序、恶意脚本植入等攻击形成全链路的管理。作为强调安全左移、持续集成的代表性服务商之一，Aqua针对开源环境下镜像、docker容器运行时场景，持续提升安全态势可视化能力，强化安全运营方案。

- 部署难度略高
- 第三方兼容待提升

❑ **VMware：**在管理Kubernetes应用全生命周期方面，VMware最早强调在应用部署前对风险进行分析和控制，支持开发早期文件的扫描和漏洞可视化呈现。在安全与开发运维协同方面，VMware通过前置安全功能，助力用户实现跨团队的风险识别、漏洞修复协作。

境外服务商相对优势

①：境外服务商在整体技术栈层面具备较为显著的创新力，在特定漏洞研究以及技术栈升级等方面始终处于领先的地位。境内服务商逐渐通过原厂研究、独立实验室孵化等方式加快技术栈发展速度。

②：在采用安全运营管理新技术或对技术进行较大变革时，境外服务商能够为用户提供较好的服务支撑。

③：境外服务商在主机安全侧偏向于技术孵化，相对而言，境内服务商偏向于进行技术转化以及后期服务交付。境外服务商率先结合镜像扫描与运行时安全监测两个环节，并对全球安全产业输出技术理念。

④：境外服务商可提供一整套安全逻辑，推动用户适应安全视角的运行逻辑，并在此基础上提供相应的服务支撑。相对而言，境内服务商更多采取适应用户逻辑拓展安全产品覆盖面的模式。

境内服务商相对优势

①：尽管在云原生技术方面，境内服务商多以贴合、跟进境外主流技术为主，但通过对境外核心技术进行分解或根据自有产线进行延伸，境内服务商更能根据境内安全环境、业务环境构建服务模式。

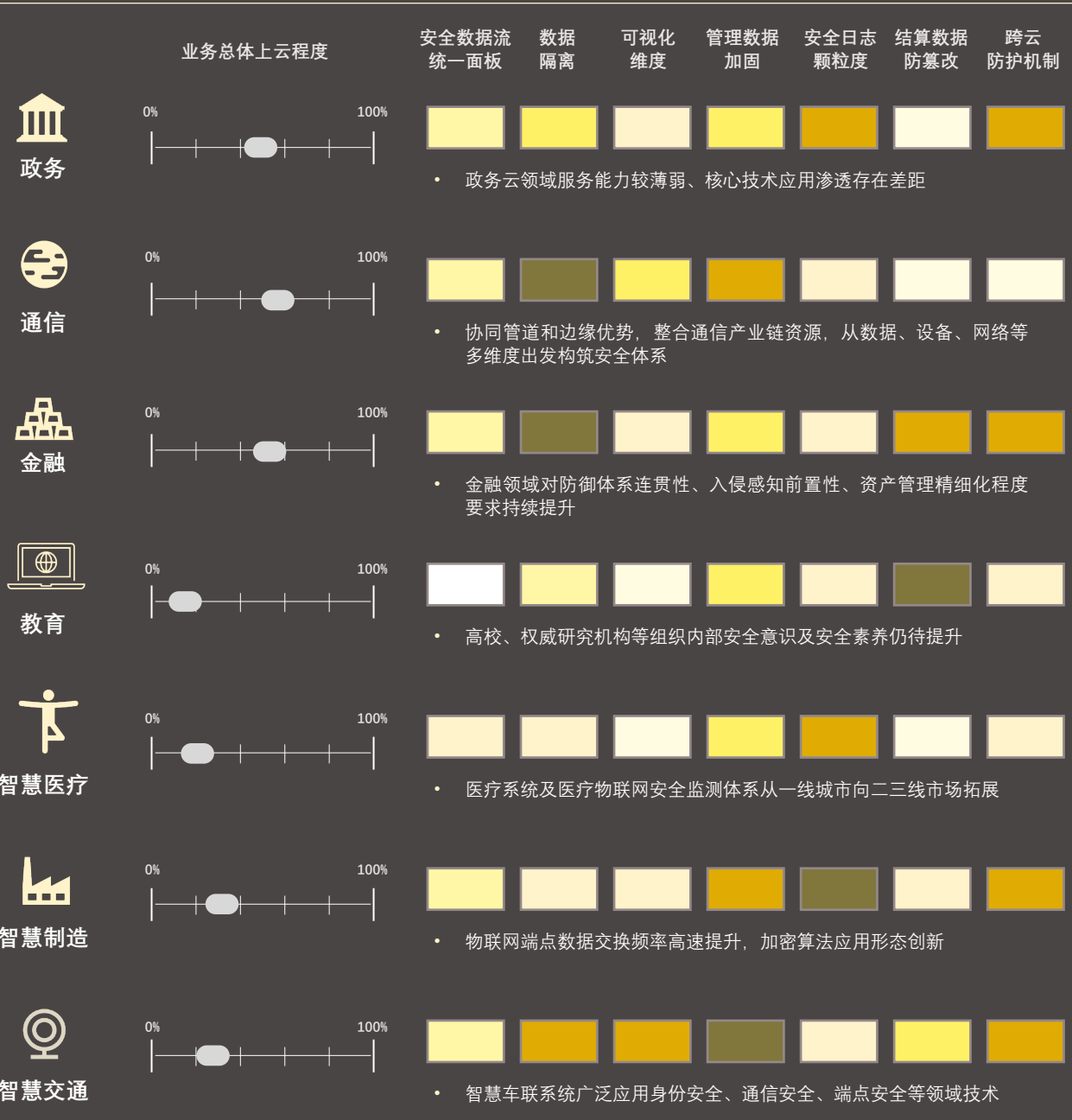
②：境内服务商在中国市场占有较为庞大的用户群体，快速推动新型安全产品线渗透，并具备较好的客户基础和商业渠道。相对而言，境外服务商当前在中国市场所部署的支持网络较为稀疏，服务推进力度较小。

章节三　用户特征观测

- 随着云主机安全用户群体业务上云加速，用户在安全数据统一面板、数据隔离、安全数据可视维度细化、结算数据防篡改、安全日志颗粒度细化、跨云防护机制等方面诉求显著性亦存在差异。

3
云主机安全用户需求特征观测

图7：不同领域用户对云主机安全产品及服务重点诉求显著性



- 云工作负载安全用户在技术选型方面的诉求逐渐呈现出针对性强、颗粒度细、贴合云原生等特征。

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，从纵深防御、快速响应、轻量化部署等领域着手，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，不构成任何证券或基金投资建议。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，概不构成任何广告或证券研究报告。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。本报告所载的资料、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，头豹可发出与本报告所载资料、意见及推测不一致的报告或文章。头豹均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。

深度研究小组负责人
李庆
13149946576
livia.li@frostchina.com

www.frostchina.com ; www.leadleo.com
https://space.bilibili.com/647223552
https://weibo.com/u/7303360042

©弗若斯特沙利文咨询（中国）
©头豹研究院