FROST & SULLIVAN
沙利文

头豹
LeadLeo

2023年
中国云原生安全市场报告

重点关注：安全体系、容器安全、集群安全、云平台安全服务

2023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云计算系列报告之《2023年中国云原生安全市场报告》年度报告。本报告旨在分析中国云原生安全服务应用市场的现状、应用前景、技术动向及发展趋势，并探析云原生安全市场竞争态势，呈现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、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原生安全应用趋势分析亦反映出云原生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原生安全市场发展周期。

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。

研究框架

图表目录

章节一
中国云原生安全市场综述

- 云原生分层多级的架构助力企业用户实现更加灵活可扩展的业务形态，但随之而来的资产暴露面增加、配置环境复杂、通讯机制变化都造成更多潜在的安全风险。
- 云原生安全能力需要与云原生基础设施架构形成完善的对应关系，针对云上工作负载平台、云网络层、容器和集群、容器编排管理系统、基础设施代码、镜像、应用程序等不同的板块形成灵活并精准对应的安全检测、防护手段，缩小云原生架构下的资产暴露面。

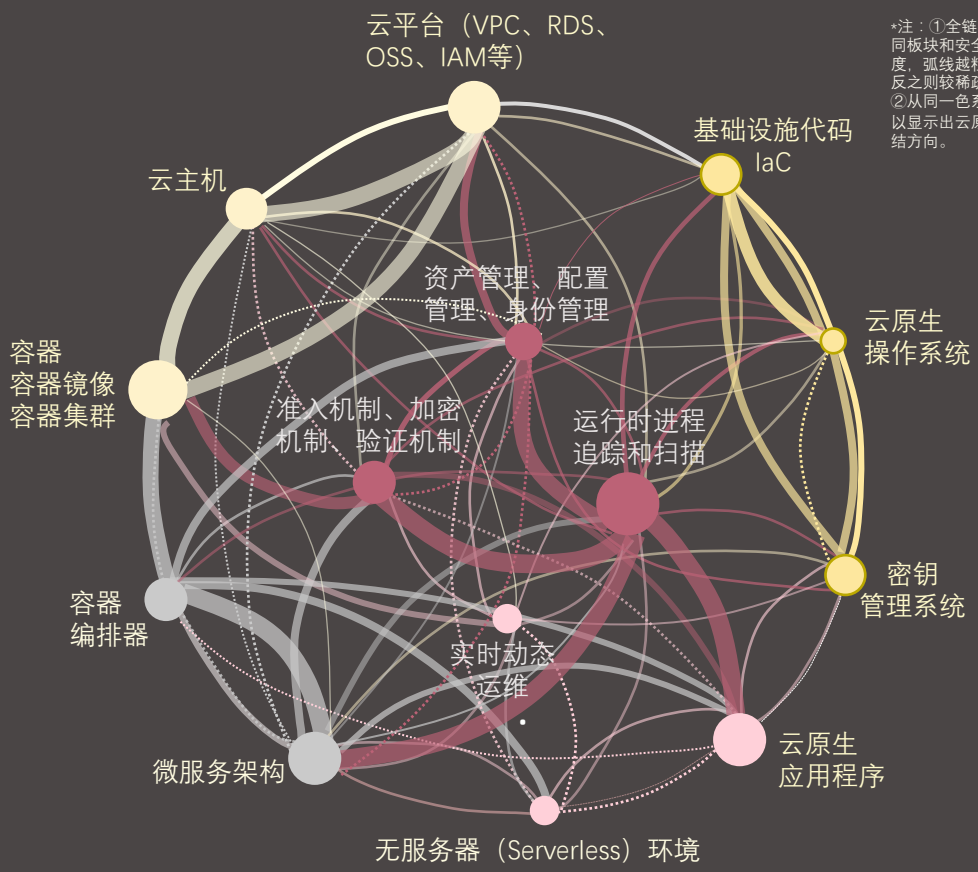
1.1 云原生安全基础架构

❑ **基础设施计算和运行颗粒度细化，云原生安全模块需灵活随航**

云原生架构在为公有云、私有云和混合云环境带来弹性可扩展的动态工作环境的同时，也为资产安全、数据安全带来新的挑战，针对云原生架构下的容器、服务网格、微服务、基础设施、声明式API等核心组成，安全服务商需要以不同于传统网络安全的思路进行云安全防护能力的构建和调优，助力最终用户在获得分布式、弹性扩展、敏捷部署、多元耦合等云原生优越性表现的同时，实现新架构下的开发安全、测试安全、交付安全、应用安全，并融合机器学习、深度学习技术，推动进一步的自动化安全防护。

从安全架构的角度而言，云原生安全能力与云原生架构具备清晰的映射关系，核心功能板块包括基础设施代码安全、容器安全、镜像安全、应用程序安全、集群安全、云原生数据安全等。随着基础设施计算和运行颗粒度的持续细化，云原生安全在不同层面（网络、计算、存储、应用、大数据等）所需具备的检测和防护能力也在持续细化的过程中，并将配合最终用户在建设混合云架构时的灵活选择，支持安全模块的灵活随航。

图1：云原生安全框架重点能力关联性拓扑



*注：①全链拓扑图中的弧线代表不同板块和安全能力点的联结紧密程度，弧线越粗代表联结程度越紧密，反之则较稀疏。
②从同一色系弧线的分配情况，可以显示出云原生安全能力的重点联结方向。

1.2 云原生安全用户核心诉求

❑ **基础设施快速升级造成的业务安全风险或为云原生普及造成阻力**

企业用户对于云基础设施的应用，已经从初期的初步上云发展到当前深度应用云原生架构，架构的变化带来更多的安全挑战，迁徙过程中可能面临更多潜在和实际发生的安全事件，云安全服务商需要快速针对云平台、容器、云主机、无服务器环境、容器编排器、基础设施即代码等不同的架构层部署有效的检测、监测、预测、防护、修复、溯源等能力，助力企业用户在业务效率升级的同时，避免因安全破防而造成的经济损失。

图2：云原生安全应用诉求要点

❑ **用户重视精细化的配置管理、授权机制、访问控制、加密机制**

在多数业务场景中，企业用户采取循序渐进的方式部署云原生架构，从初期评估规划到完成容器化、引入云原生技术、重建应用程序架构，整体过程面临的不同层面风险需相应的安全防护手段和工具。①云上工作负载平台是搭建云上应用程序的基础，而随工作负载激增，平台漏洞和应用程序漏洞也无可避免大幅增长，用户亟需在管理大量工作负载平台的同时实现合规配置；②在容器、镜像、集群的层面，最终用户需要安全服务商能够提供更加灵活可扩展的验证和授权控制机制，提供对容器间、集群间通讯流量漏洞和威胁的有效识别防护手段，并建立可快速规模化应用的隔离策略；③在容器编排器的层面，端口、主机等核心通讯节点的访问控制和验证的要求更为严格，用户需要确保核心操作系统、核心节点的合规访问；④在代码的层面，用户在享用一键部署便利的同时，更需精确的配置以降低资产暴露面，并执行完善的加密措施。

章节二
中国云原生安全核心板块及技术覆盖

- 云原生环境相对虚拟化的上云进程，存在架构和应用模式本质的区别，IaC、容器、容器编排系统、微服务、无服务器等模式更能发挥云计算灵活弹性的优势。
- 云原生环境下，资产激增和通讯流量复杂的特征推动安全策略的更新，云原生安全解决方案需要提供更细力度的资产、流量、配置、身份和行为管理工具，提升漏洞检测和修复的敏捷性。

2.1 基础设施代码安全板块

❑ **针对基础设施层进行合规配置实时扫描，促进安全左移的落地**

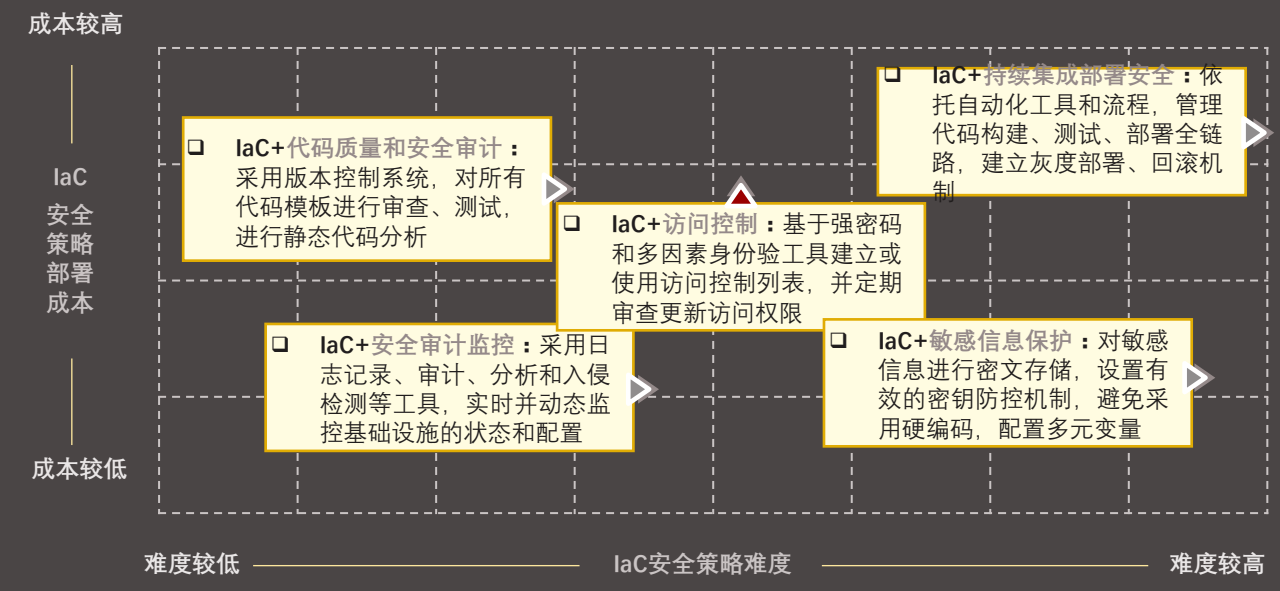
基础设施代码层面安全防护策略的建立是安全左移的代表性实践，尽管在云原生环境下，容器、镜像和集群的合规配置和安全检测、防护策略更易受到关注，但基础设施代码是云原生工作流的基础，宜建议用户重视该层面安全卡点的建设，更加严格准入策略，强化资产安全，将准入机制从容器和镜像层面左移至基础设施代码环节。

基于基础设施层配置安全性的增强、准入管理机制的建设，云原生用户可更加便捷地启用IaC命令式和声明式的脚本模板，并获得模板的可复制性、可维护性和安全性；安全服务商通过对IaC模板配置情况的持续扫描，及时发现漏洞，将风险控制在业务生产流程之前，确保CI/CD的顺利实现。

❑ **依托统一策略引擎支持基础设施代码层配置管理、密钥管理、可信管理**

当前常见的IaC风险集中在不当或者错误配置、硬编码密码导致的漏洞、敏感信息漏洞、基础镜像漏洞、对接第三方工具和库的风险、脚本代码逻辑错误或语法错误等方面。其中，镜像漏洞经过镜像再生后将以指数速度扩大，未认证镜像的漏洞难以察觉，硬编码则导致密钥被轻易探知，参照核心风险类别，云原生安全服务商能够提供针对性的IaC安全策略，包括以上提到的IaC配置持续扫描和漏洞检测引擎的开发和算法优化、可信脚本认证、IaC密钥合规管理，并依托统一的策略引擎实现整体业务环境的代码安全。

图3：IaC层安全防护策略应用特征



2.2 容器和容器编排器安全板块

容器和容器编排器构成云原生的标准化基础设施，容器和容器镜像的应用呈指数级增长，日趋复杂的底层生态对安全管控带来更多挑战，容器层面的特权账号风险、攻击逃逸风险、容器镜像漏洞皆有可能造成攻击行为在组织内部的快速渗透，容器编排器层面的不当配置或组件漏洞也将放大风险暴露面，譬如端口漏洞、关键控制节点劫持、密钥泄露或未校验凭证等，皆有可能导致底层计算资源遭到入侵。

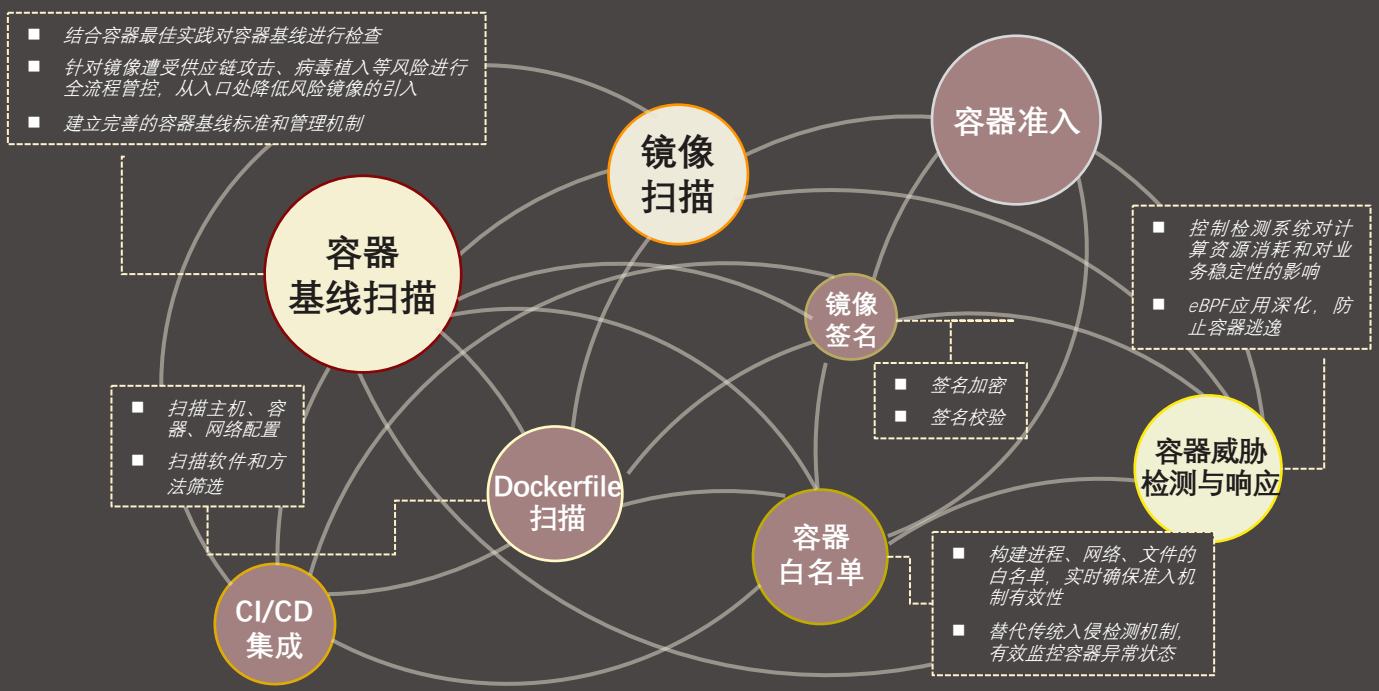
❑ **实时扫描管控，强化准入机制，确保基础设施安全**

容器层面的安全管控主要涉及容器镜像管控、建立严格准入控制机制、构建容器基线、进行签名校验等方面，服务商需对镜像仓库进行持续的风险扫描，并在入口做好合规拉取管控措施，并实时汇总镜像扫描结果，更新准入控制项目和容器基线，此外，针对容器进程、文件、网络的白名单也应加强基础设施模板的安全性、可复制性。

❑ **容器管理调度层面宜更加重视安全操作机制的落实**

容器编排器可能面临未经授权的访问、恶意提权、错误配置、恶意资源消耗、数据泄露等类型的风险，防护策略的重点可落在容器编排器访问和授权机制建设、配置维护、组件定期更新、有效的网络隔离和网络策略、有效凭证管理等方面，以确保关键业务控制节点的合理访问和操作。

图4：结合基线、动态扫描、白名单、签名等机制提升容器生命周期安全



2.3 云主机安全板块

- 云主机是承载云原生环境中所有工作流量的基底，可能存在因基线配置失当、资产档案缺失而产生的漏洞或端口暴露风险，在遭受攻击和入侵的情况下，云主机的失陷可能传导至整个云平台，在混合云环境下，则可能面临更加复杂的风险传导效应。

云上资产清点

云主机安全层面的基础能力在于安全检查和安全运维，具体包括资产清点、资产权限配置、日志管理等工具和框架，云原生资产形态与虚拟机资产形态存在量级和结构方面的差异，需要对容器实例名称、配置、状态和所属的应用程序或服务进行全面清点，同时对存储资源、网络、身份凭证、自动化工具脚本、第三方工具等资产类别进行实时管理。

云上合规基线配置

云原生环境下，基线配置涉及身份和访问管理、网络安全组、敏感数据、日志记录监控、操作系统和应用程序、漏洞和补丁等方面，可依托强密码策略、流量限制、加密算法升级、密钥管理升级、预警和响应机制设计、安全补丁应用和更新等策略，在确保对通用基线部署的同时，提供更多自定义基线设置的维度，细化基线管理颗粒度。

云上病毒发现机制演进

防病毒引擎的搭载为整体云上业务流程增加了流量负担，占用较大运行资源，鉴于云上工作负载运行周期较短，传统分析训练型的防病毒机制开始转向异常情况应对机制，服务商可在确定可信进程、数据、文件等资产后，采用白名单策略，阻断一切形式的异常状态，并且对存在病毒的云主机资源采取分类检测响应策略。

云上网络隔离

云上工作负载环境下，业务进程共享操作系统内核，更加容易产生容器逃逸现象，安全服务商需助力企业用户做好网络隔离，具体可通过创建网络逻辑隔离、虚拟私有云、子网划分和进程分配、配置虚拟防火墙、在子网级别建立访问控制列表、应用服务网格、采用TLS/SSL协议进行流量加密等方式，细化流量管理和网络隔离策略的颗粒度。

2.4 云原生微服务安全板块

- 微服务架构的应用是云原生安全区别于传统业务上云模式的重要特征之一，而应用程序在被拆分为更多服务模块的同时，也带来资产规模快速增长、流量追溯困难等现象，这对云安全服务商带来更多的挑战，也带来重塑安全架构的机遇。

❑ 微服务的应用让应用系统的编写和更新更趋灵活敏捷

云原生架构下的微服务模块在本质上亦为应用程序组件，在形式上将复杂的应用程序拆分为多个服务模块，并在服务模块之间通过API进行计算指令的传递，拆分后的微服务模块为开发人员提供了更大便利，支持不同开发语言的编写，且在整体上构成应用系统。鉴于服务模块的拆分，微服务架构能够助力开发人员以更灵活的方式更新应用程序，在云原生环境下实现服务模块的滚动更新和灰度发布，以及回滚。

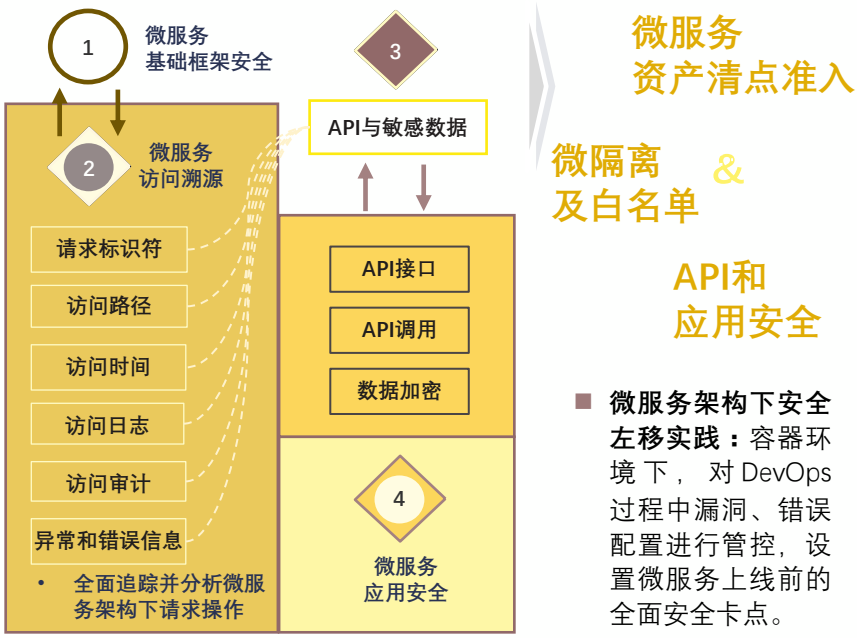
微服务架构在全球开发环境中迅速普及，并且衍生出无服务器（FaaS）框架，助力企业开发人员能够更加专注于业务本身的特征和开发诉求，从传统开发环境的限制和低效状态中解脱出来。尽管微服务架构支持更好的拆分和更有序的故障管理（熔断、限流等策略），随之而来的不同于传统开发运维环境的安全挑战也快速增加。

❑ 构建微服务级别的资产管理、流量管理和身份管控安全体系

鉴于微服务框架对应用程序更细颗粒度的拆分，随之而来的是攻击面的规模化增加，微服务模块之间通过API进行通讯，需要对流量访问和行为授权进行管理的卡点增加，此外，规模化的服务模块增加也为应用系统内整体流量动向的梳理和追踪带来巨大挑战，单个服务模块的失陷可能导致攻击在系统内部和向系统底层的迅速蔓延，进而导致数据泄露、远程控制等风险，此外，开发环节也存在错误编码、硬编码等风险。

针对微服务框架的特征，云原生安全解决方案需要提供针对微服务级别的资产清点和关系动态图谱，通过强化扫描策略的方式加强微服务资产的准入管理，此外， 通过采用零信任机制、白名单机制等方式有效控制访问和进行行为授权。

图5：微服务架构下DevOps全流程安全管控和卡点定位



■ **微服务架构下安全左移实践：**容器环境下，对DevOps过程中漏洞、错误配置进行管控，设置微服务上线前的全面安全卡点。

章节三
中国云原生安全市场发展机遇

3.1 场景拓展机遇-多元产业加速上云

3.2 应用升级机遇-融合AI/ML工具

- 企业在数字化转型进程中，经历了从硬件设备到虚拟化云平台，再到云原生的不同阶段，云计算应用和进程的分配从基础设施层系统层面上升到云系统层面，同时要求更细颗粒度的服务和服务间通讯安全能力。
- AI技术与云原生安全之间具备双向驱动的作用，AI技术助力安全平台更有效地利用日志、威胁情报、漏洞等数据，提升安全检测防护效率，而云原生安全能力助力AI供应链实现全面风险管理，构筑更加高效的AI平台。

3.1 场景拓展机遇-多元产业加速上云

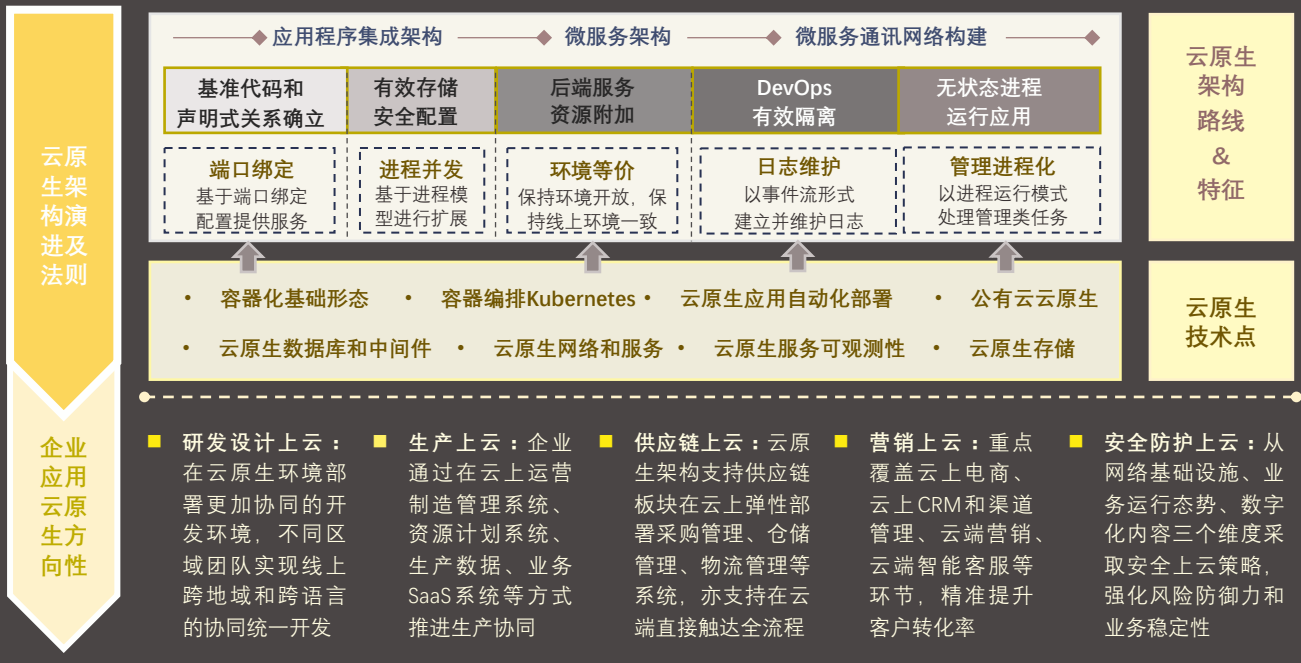
> “云原生应用的趋势不仅仅，也不主要是一种技术趋势，云原生应用的趋势更多是一种文化和组织变革的趋势。”
>
> ——云原生架构创始人Matt Stine

随着各行各业企业业务上云部署的进程发展，数字化业务对IT资源的可扩展性、敏捷性、灵活性要求快速提升。在传统上云模式下，计算资源从硬件设备迁徙至虚拟化的系统中，但本质上仍然以设备为资源分配的基础，无法满足数字化业务对IT资源指数级增长的需求，而云原生架构的应用进一步将虚拟化计算资源作为基础算力总控平台，构建对应用系统的直接支持。当前企业应用云原生架构的关键技术要素包括四方面。

1. 微服务：作为可独立部署、独立开发的服务模块，处理特定的业务功能，对扩展和维护更加友好，多个微服务模块构成应用程序系统；
2. 容器化：通过容器化的应用进程，实现不依赖于运行环境的业务进程；
3. DevOps：基于云原生架构松耦合的特征，实现持续迭代和自动运维；
4. 持续交付：将应用交付自动化，支持滚动部署、灰度部署、回滚等能力。

毋庸置疑，云原生技术的应用帮助企业更好地应对业务爆发式增长的过程，从开发、交付、部署、运维等不同角度带来便利和稳定性，云原生架构对云上资源更细粒度的分配帮助企业用户降低用云成本，将企业发展的重心更加集中于业务本身。

图6：云原生结构推动企业多元系统实现运维降本和效率转化



3.2 应用升级机遇-融合AI/ML工具

在云原生架构下，安全服务商可借助快速迭代突破的AI能力实现对开发、部署、运维的无缝安全管理和安全功能渗透，具体应用方向包括智能化SASE平台建设、AI供应链管理、安全中心自动化运营、运维安全自动化等。

❑ **SASE平台借助AI技术实现统一管理和自动化运维**

SASE平台能够为公有云、本地数据中心、移动端、SaaS、云计算基础设施等提供统一网络安全能力和服务，在AI技术的驱动下，SASE平台能够对安全功能、网络功能相关数据进行全盘管理，并通过统一管理模式在微服务组件和进程等层面实现AI运维。

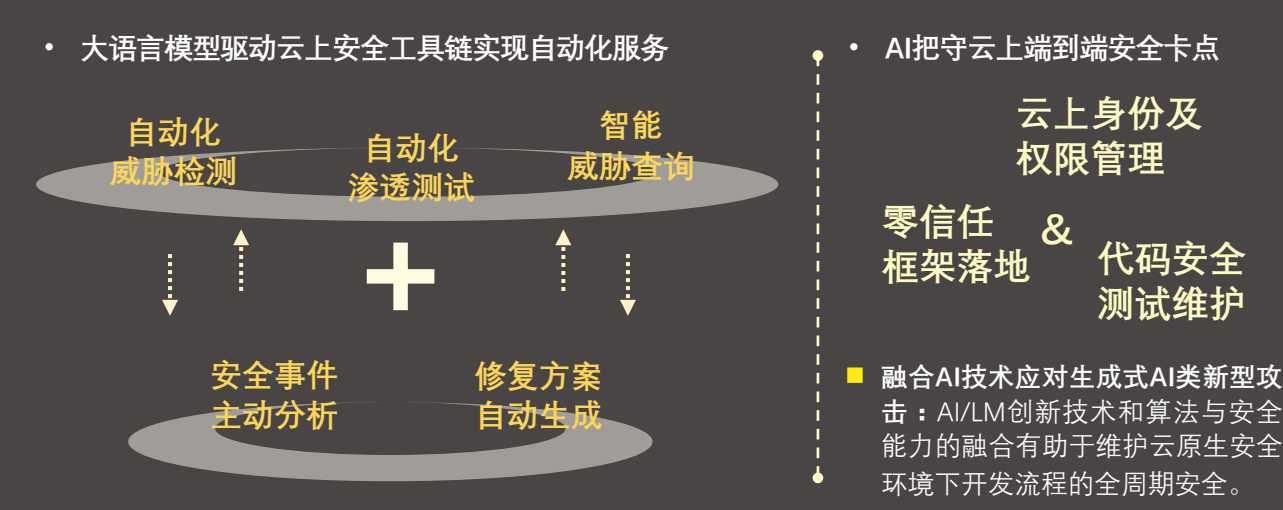
❑ **云原生安全平台框架与AI供应链管理具备高适配性**

云原生安全防护平台融合安全态势管理、云服务网络安全、云工作负载安全等核心板块，可为AI供应链提供更细颗粒度的的安全防护能力以及动态合规配置服务，助力AI开发企业实现更加安全的供应链和人工智能应用。

❑ **日志、威胁情报、告警数据颗粒度细化，实现快速安全检测和分析**

云原生安全不同层面的日志统计和告警能力需要融合AI技术，推动细粒度数据收集训练，进而提高告警数据交叉关联、快速应对复杂威胁、快速判断攻击面、自主响应等能力，进一步缩短漏洞检测周期，推动安全前置。

图8：云原生安全工具链多维度融合AI和大模型



- 大语言模型为云原生安全体系增强和补充可用工具和关键流程，在估计低层次任务安全性的同时，从自动化威胁检测、攻击事件数据主动分析、自动化修复方案生成、自动化渗透测试脚本处理等方面提供无缝安全方案。

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，从云原生架构、云工作负载安全、云上开发部署安全等领域着手，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。

头豹 LeadLeo

FROST & SULLIVAN 沙利文