中国云原生安全用户调查报告（2023 年）

云原生产业联盟

2023 年 12 月

前言

2022 年全球云计算市场规模为 4,910 亿美元，增速 19%，预计在大模型、算力等需求刺激下，市场仍将保持稳定增长，到 2026 年全球云计算市场将突破万亿美元。2022 年我国云计算市场规模达 4,550 亿元，较 2021 年增长 40.91%。相比于全球 19%的增速，我国云计算市场仍处于快速发展期，预计 2025 年我国云计算整体市场规模将突破万亿元。随着全行业上云进程的深化，云原生技术凭借其敏捷、弹性、可编排、高可用等优秀特性成为企业实现数字化转型的重要途径。然而，云原生对传统信息技术架构和应用模式的颠覆性改造引入了新的安全风险，云原生架构安全、容器安全、安全运营等问题受到重点关注。为进一步掌握中国云原生用户的使用状况和特点，云原生产业联盟开展了 2023 年度中国云原生用户使用状况的调查。本次活动采用在线调查的方式，共回收有效问卷 648 份。本报告以调查结果为基础，结合行业专家的深度访谈，力争详实客观地反映云原生用户安全需求，为广大关注云原生安全产业的从业人员、专家学者和研究机构提供真实可信的数据支撑。

本次报告的编写以及数据采集工作得到了阿里云、悬镜安全、默安科技、奇安信、绿盟科技、小佑科技、青藤云安全、厦门服云、安恒信息、深信服、创原会、华为开发者联盟、瑞数信息以及社会各界的大力支持，在此谨表示最衷心的感谢！同时也对接受云原生用户调查访问的用户朋友表示最诚挚的谢意！

观点摘要

用户云原生应用及技术建设现状

- **云原生技术成为企业云支出重点投入方向。**15.92%的用户云原生支出占云总体支出比例（包含研发、运维、采购）低于 10%，35.7%的用户云原生支出占云总体支出比例为 10%~30%，29.06%的用户云原生支出占云总体支出比例为 30%~50%，19.32%的用户云原生支出占云总体支出 50%以上。
- **容器技术得以广泛应用，9 成以上用户已经使用或计划使用容器技术。**50.71%的用户已将容器技术用于核心生产环境，27.5%的用户已将容器技术用于次核心生产环境，15.05%的用户正在评估测试使用容器技术，5.19%的用户正对容器技术进行评估考虑，仅 1.55%的用户未考虑使用容器技术。

用户云原生安全建设现状

- **云原生规模化应用时的安全性、可靠性和连续性成为用户使用云原生技术的最主要顾虑。**在选用云原生技术时，有 81.91%的用户对云原生技术在大规模应用时的安全性、可靠性、性能、连续性心存顾虑（较 2022 年该百分比上升 10.17%）。
- **云原生安全价值需求日益凸显，近 9 成企业已经开展或计划开展云原生安全建设。**仅有 10.36%的用户不计划部署云原生安全工具和相关产品，32.77%的用户已经部署并长期维护云原生安全工具或相关产品，12.67%的用户已经部署并考虑升级、更新相关工具和产品，44.6%的用户计划未来一年内部署云原生安全技术工具和相关产品。
- **云原生攻击手段愈发多样，云原生基础架构为主要攻击目标。**针对集群错误配置及权限攻击占比达到 32.74%，容器网络攻击、容器入侵攻击，以及镜像漏洞和镜像投毒占比分别为 25.41%、24.65%、 25.25%。2023 年，用户也曾遭遇暴力破解攻击、内存马

攻击、微服务应用攻击、CI 流水线被劫持、凭据泄露、组件级供应链安全等问题，分别占比 22.10%、18.39%、18.09%、15.30%、12.98%、3.40%。

- **用户对暴露面管理、安全运营的关注度显著提升。**调查显示，今年关注安全运营的用户占比首次超过三成，30.18%的用户表示关注安全运营。同时，用户对于整体云原生安全的暴露面管理也更加关注，此类用户占比 23.8%。此外，用户对容器安全关注度仍然很高，64.47%的用户关注容器运行时安全，58.02%的用户关注容器网络安全。

云原生安全关键能力建设

- **云原生基础设施配置的风险检测是云原生环境下云安全运营的基本需求。**在云原生环境下，42.66%的用户表示云上安全运营需要做好云原生基础设施配置的风险检测。另外，34.05%的用户希望云上安全运营具备多云、混合云环境下安全态势的统一管理。30.96%的用户认为在云原生环境下，攻击面进一步扩大。
- **CIS 基线规范与国内应用场景不符，国内基线规范研发价值凸显。**当前 57.21%的用户依然使用 CIS 规范，41.76%的用户使用内部设计规范，仅有 1.03%的用户使用国内的基线规范标准。但是数据显示，未来有 57.24%的用户计划使用国内标准为内部安全基线规范 32.57%计划使用自主设计规范，10.19%的用户计划采用 CIS 规范。

云原生安全建设趋势

- **云原生安全向原生化、一体化、智能化不断演进。**60.12%的用户未来会推动安全服务云原生化，使安全服务更加敏捷灵活；50.19%的用户未来会建设适配多云环境的一体化安全平台；40.12%的用户未来会增强智能化安全防护，将 AI 技术融入安全防护全流；仅有 24.84%的用户未来计划借鉴 CNAPP 安全框架，补足自身安全短板。

一、调查背景

（一）调查方法及样本

1、调查方法

本次调查采用在线调查的方式，共收集到有效问卷 648 份。

2、样本描述

参与调查用户所在行业：包括金融、互联网、政府、制造、能源、电信、建筑、轨道交通、科教文卫，以及其他行业。

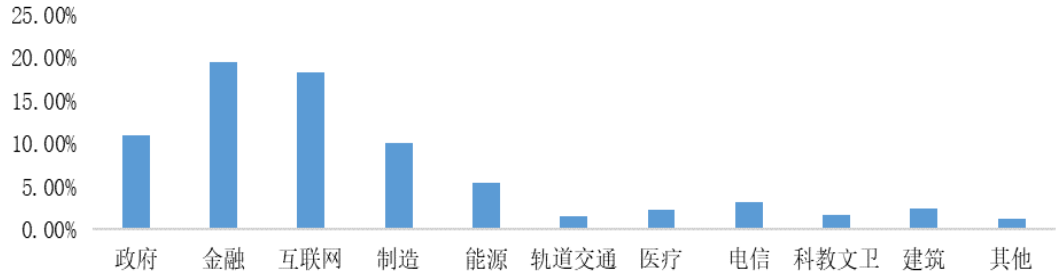

图 1 调查用户的行业分布

参加调查用户所在企业的规模：共分为 1-100 人、101-500 人、501-1000 人以及 1000 人以上四档。

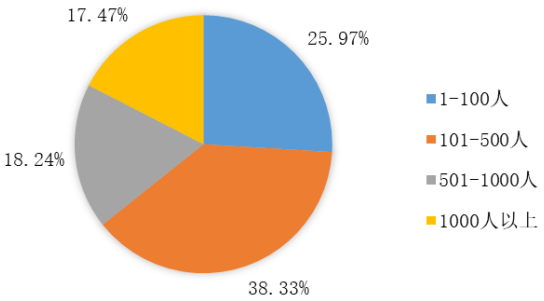

图 2 调查用户所在企业的规模

受访者在公司中主要担任以下角色：产品/运营人员、安全运维工程师、销售/市场人员、软件经理/总监、研发工程师、非技术领导（如 CEO、COO、CMO、CRO 等）、技术线领导（如 CTO）。

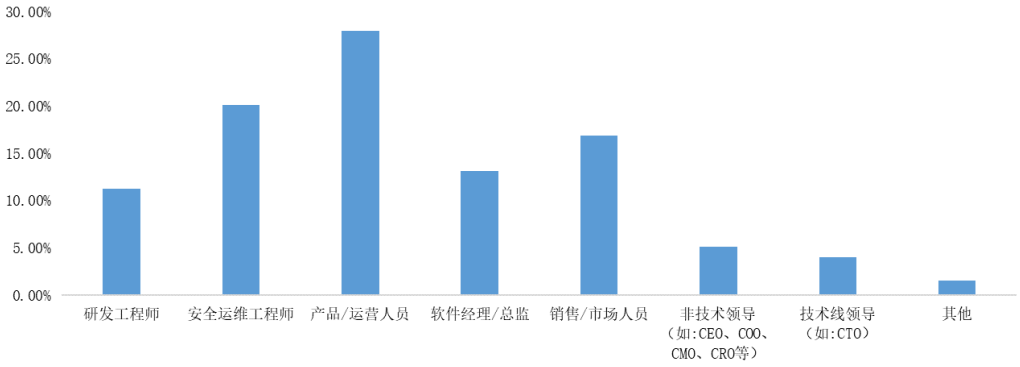

图 3 受访者在公司担任的角色

二、云原生应用及技术建设现状

（一）云原生建设支出情况

企业加强云原生建设投入，近 2 成用户云原生支出占云总体支出 50%以上。今年的调查数据显示，已有相当一部分用户正将云建设的中心转向云原生，近三成用户云原生支出占云总体支出超 50%。从调查数据来看，仅有 15.92%的用户云原生支出占云总体支出比例低于 10%，35.7%的用户云原生支出占云总体支出比例为 10%~30%，29.06%的用户云原生支出占云总体支出比例为 30%~50%，19.32%的用户云原生支出占云总体支出 50%以上。

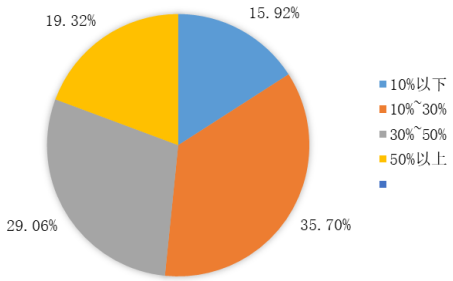

图 4 云原生占云总体支出比例

（二）容器采纳率

容器在生产环境中的采纳率逐年攀升，用户认可度进一步增强。50.71%的用户已将容

器技术用于核心生产环境，27.5%的用户已将容器技术用于次核心生产环境，15.05%的用户正在评估测试使用容器技术，5.19%的用户正对容器技术进行评估考虑，仅 1.55%的用户未考虑使用容器技术。

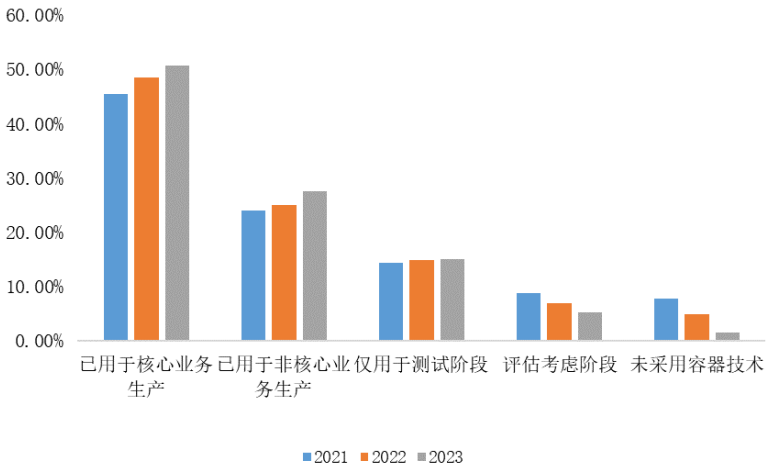

图 5 容器技术采纳情况

三、云原生安全建设现状

（一）云原生安全应用现状

规模化应用的安全性、可靠性和连续性仍旧是用户选择云原生的主要疑虑。2022 年数据显示，用户云原生技术大规模应用下的安全性、可靠性和连续性是用户选择云原生技术的主要顾虑，2023 年来看这种顾虑仍旧存在并且有扩大趋势。从调查数据来看，81.91%的用户对云原生技术在大规模应用时的安全性、可靠性、性能、连续性心存顾虑，46.83%的用户认为云原生技术栈过于复杂导致学习成本高，34.4%的用户担心云原生技术应用与现有的研发/测试/运维平台/流程整合演进不匹配，29.88%的用户认为云原生迁移难度大、成本高、迁移效果不可预测，仅有 15.61%的用户认为云原生应用价值不明显、投入产出比有待评估。

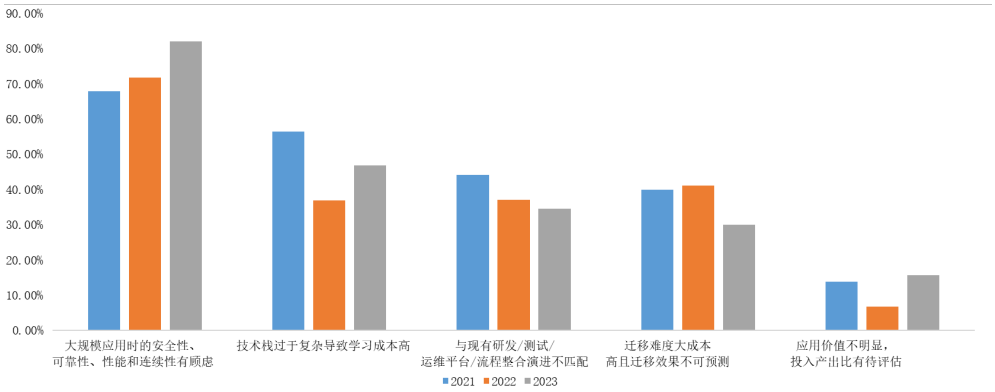

图 6 用户采用云原生技术时存在的顾虑

云原生安全价值需求日益凸显，近 9 成企业已经开展或计划开展云原生安全建设。随着云原生技术的深化应用，其技术架构和应用模式的持续变革也引发了新的安全风险和挑战，云原生安全逐步成为用户关注焦点。据调查数据显示，2023 年已有 32.77%的用户已经部署并长期维护云原生安全工具或相关产品，12.67%的用户已经部署并在考虑升级、更新相关工具和产品，44.6%的用户计划未来一年内部署云原生安全工具和相关产品，仅有 10.36%的用户不计划部署云原生安全工具和相关产品。

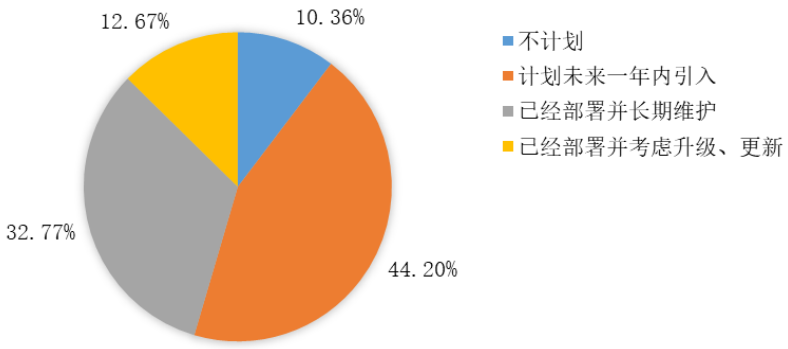

图 7 云原生技术工具和相关产品的计划建设情况

研发运维共同参与仍然是云原生安全建设的主要方式。 现阶段，由于云原生安全依然是新兴的交叉技术领域，需要云原生技术与安全的跨界融合，所以研发与运维共同参与以解决云原生架构下的安全风险依旧是云原生安全建设的主要方式。在本次调研中，仅有 12.98%

的用户所在企业是由独立的信息安全部门来处理云原生安全问题，41.27%的用户由运维部门与开发部门同时承担云原生安全的运维工作，16.07 %的用户由云计算运维部门担任云原生安全运维工作，28.44 %的用户由业务开发部门负责。

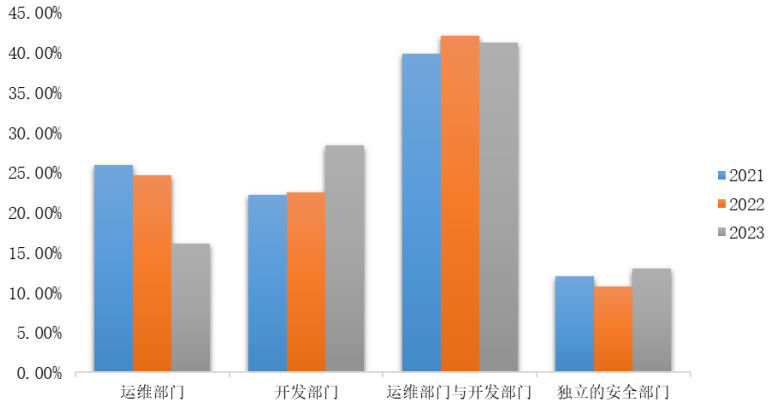

图 8 云原生安全建设的参与部门

技术门槛高和人力成本高是企业云原生安全建设面临的主要挑战。云原生安全技术作为一种新兴的交叉技术，面临着技术复杂、门槛较高问题，由此也会导致相关人才的缺失和人力成本高等现状。据调查数据显示，54.57%的用户表示云原生技术门槛相对较高，48.28%的用户认为云原生安全建设人力成本高，45.64%的用户认为云原生安全建设缺乏整体的安全解决方案，38.69%的用户认为在多云、混合云环境下安全能力的集成困难是云原生安全建设的难点， 19.78%的用户认为需求不明确是云原生安全建设的问题，23.65%的用户表示云原生安全建设面临的主要挑战是多部门沟通成本高。

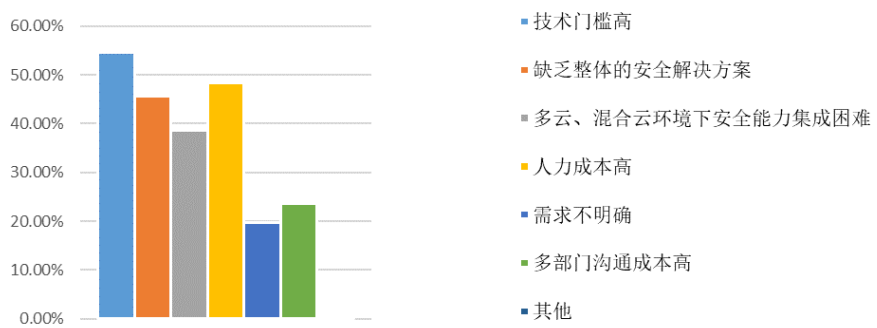

图 9 云原生安全建设过程中遭遇的挑战

（二）云原生安全能力建设现状

云原生攻击手段多样化，针对集群的攻击事件占比较多。随着企业上云用云进程的深入，针对云原生环境的攻击手段也层出不穷，调查数据显示 2023 年，用户遭遇了多种类型的云原生安全事件，仅有 6.96%的用户表示没有遭遇过云原生安全事件。集群、容器、镜像仍然为攻击者主要攻击对象，其中集群错误配置及权限攻击占比达到 32.74%，容器网络攻击、容器入侵攻击，以及镜像漏洞和镜像投毒占比分别为 25.41%、24.65%、 25.25%。此外，2023 年，用户也曾遭遇暴力破解攻击、内存马攻击、微服务应用攻击、CI 流水线被劫持、凭据泄露、组件级供应链安全等问题，分别占比 22.10%、18.39%、18.09%、15.30%、12.98%、3.40%。

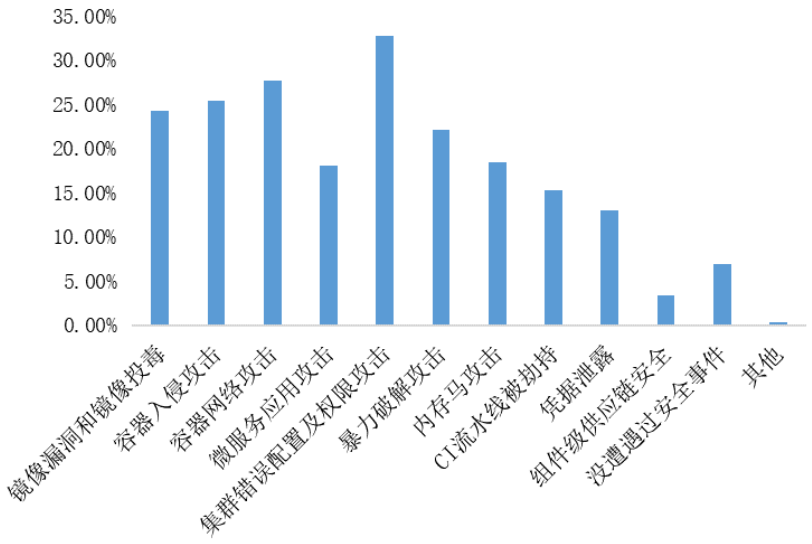

图 10 2023 年用户遭遇的云原生安全事件类型

用户重点围绕制品安全、容器安全、网络安全等开展云原生安全能力的建设。与 2022 年调查结果对比可以看出，2023 年用户提升了云原生安全各个方面的能力建设。其中，云原生网络入侵检测能力、镜像安全扫描能力、集群的安全监控与审计能力、容器运行时检测能力依然是用户优先建设的云原生安全能力，分别占比 50.88%、38.7%、38.02%、35.46%。

除此之外，2023 年用户重点加强了 CI/CD 中自动化制品安全检测能力的建设，已有 33.54%用户具备该能力，相较于 2022 年 8.97%的占比，该能力占比提高了 24.57%。此外，已有 29.72%的用户具备细颗粒的网络访问控制能力，25.63%的用户具备微服务应用安全能力，18.39%的用户具备 API 安全防护能力，10.05%和 17.02%的用户已具备 serverless 安全保护能力和数据安全能力。

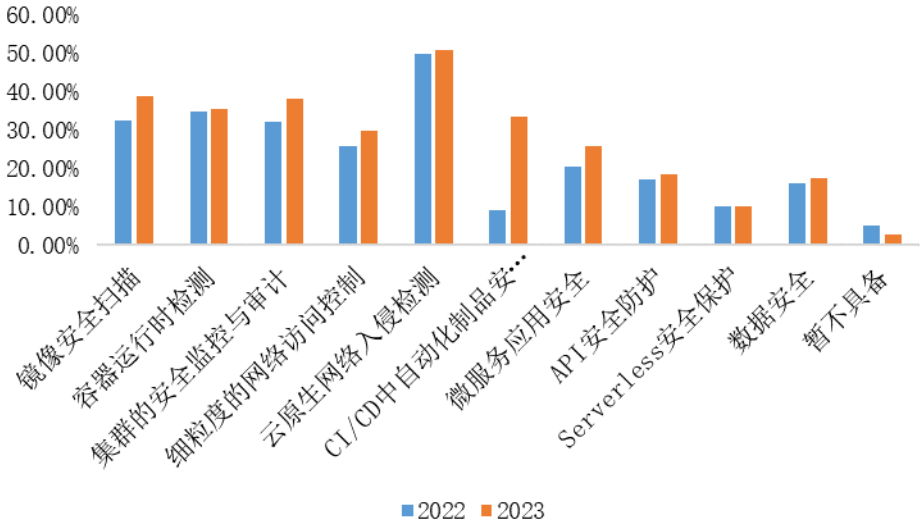

图 11 企业云原生环境下已具备的安全能力

用户对容器运行时安全、容器网络安全关注度依然不减，同时对暴露面管理、安全运营的关注度显著提升。2023 年依然有超过六成的用户关心容器运行时安全，同时，用户对于安全运营和暴露面管理的关注度大幅提升。调查显示，64.47%的用户关注容器运行时安全，58.02%的用户关注容器网络安全。此外，关注安全运营的用户占比首次超过三成，30.18%的用户表示关注安全运营。同时，用户对于整体云原生安全的暴露面管理也更加关注，此类用户占比 23.8%。另外，依然有 28.94%用户关注微服务应用安全，制品安全方面，镜像安全扫描占比与 2022 年基本持平，占比 39.2% ，CI/CD 流程中自动化制品安全检测关注度有所提升，占比 25.55%。此外，12.21%的受访者关注容器编排引擎安全，12.21%的受访者关注数据安全，19.01%的受访者关注 API 安全，16.12%的用户关注 serverless 安全。

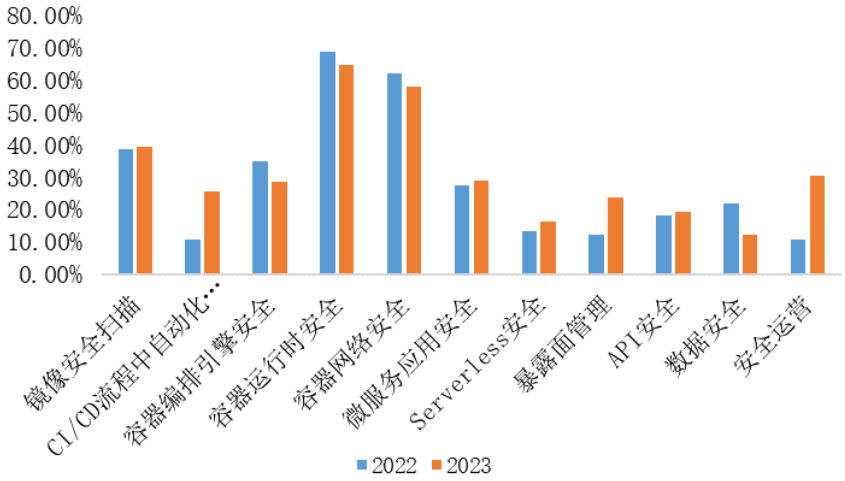

图 12 企业关注的云原生安全能力

（三）云原生安全工具使用现状

自动化测试工具在 CI/CD 安全中持续发挥重要作用，IaC 扫描工具使用率显著提高。

在云原生环境中，容器的整体生命周期通常较短，并且在大规模应用中容器数量往往很庞大，这导致容器的风险检测成本增加、误报率上涨，增加了安全团队的运维工作，导致安全运维效率变低，无法满足云原生应用敏捷开发、高速迭代的需求。因此，用户需要更加自动化和智能的工具以更早地识别和理解问题，并更快地修复问题。根据调查结果显示，50.39%的用户使用了镜像扫描工具，44.67%的用户使用了动态应用程序安全测试(DAST)，33.28%的用户使用了基础设施即代码（IaC）扫描工具，35.97%的用户使用了静态应用程序安全测试(SAST)，23.34%的用户使用了风险镜像控制与阻断工具。仅有 12.94 的用户暂未在 CI/CD 流程中引入安全工具。

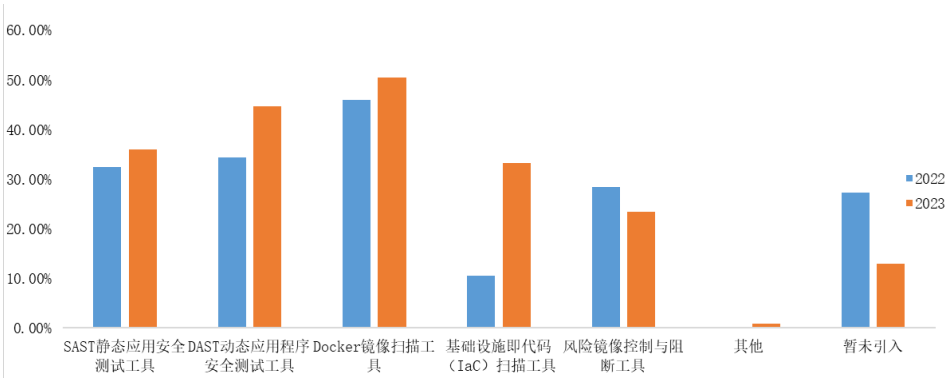

图 13 CI/CD 流程安全工具使用情况

容器级别的网络控制仍是企业主流的网络安全访问控制措施。在云原生网络安全方面，73.99%的用户通过 Calico 等组件做容器级别的网络访问控制，使用宿主机之间的 ACL 网络访问控制占比 66.03%，同时有 46.41%的用户使用服务网格进行访问控制，使用微隔离产品占比 9.58%。

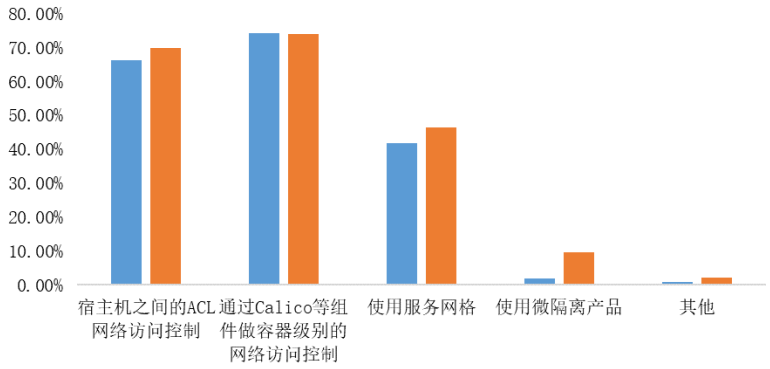

图 14 网络访问控制产品使用情况

云原生应用安全工具使用率显著提高。与 2022 年数据相比，用户云原生应用防护工具使用率明显增高，使用的工具类型也更加多样化。2023 年，仅有 2.01%的用户暂未使用云原生应用防护工具（较 2022 年百分比下降 22.99%）。其中，API 应用网关、API 安全监控和应用漏洞扫描工具使用占比排名前三，分别占比 41.22%、30.91%、31.89%，同时 27.84%的用户使用了拒绝服务防护网关，25.81%用户使用 eBPF 可观测产品，23.03%的用户使用了云 WAF，使用 Bots 检测防护产品的用户占比 19.52%，应用层国密套件使用占比 12.06%，安全威胁大数据分析产品占比 8.66%。

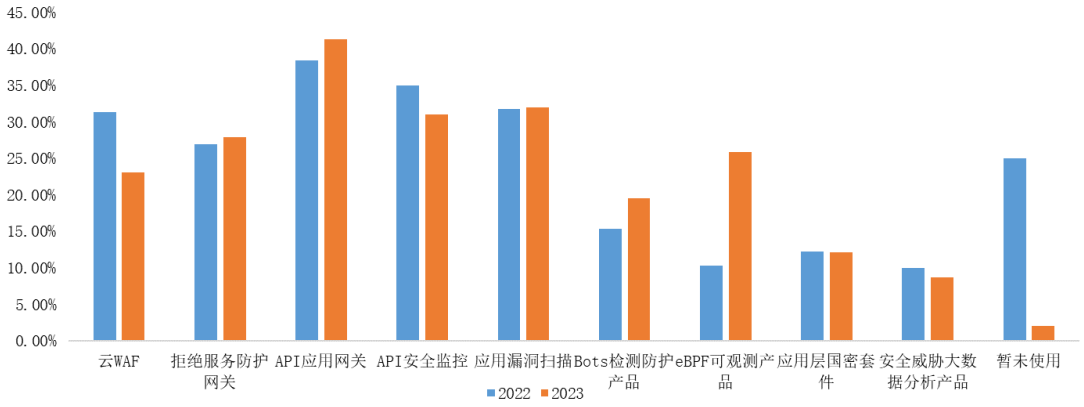

图 15 2023 年云原生应用防护工具使用

超过 70%的用户表示在实际生产环境中使用 5 个及以上的云原生安全工具。现阶段用户愈发重视云原生安全能力建设，但由于云原生安全防护体系庞大，现有云原生安全产品大多仅聚焦单个或几个细分领域，导致企业云原生安全工具使用量激增。据调查数据显示，26.12%的用户表示在实际生产环境中使用 5 个以下的云原生安全工具，38.64%的用户表示在实际的生产环境中使用 5~10 个云原生安全工具，22.10%的用户表示使用 10~20 个云原生安全工具，13.14%用户在实际生产环境中使用 20 个以上的云原生安全工具。

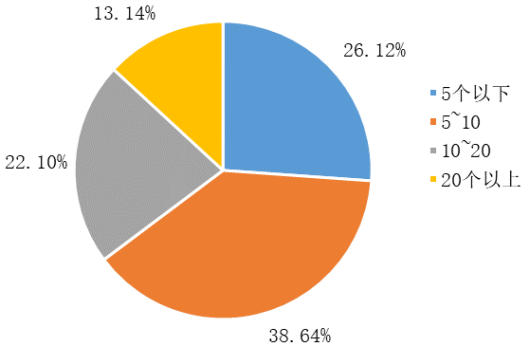

图 16 用户使用的云原生安全工具数量统计

一体化的云原生安全应用保护平台在未来有望成为主流。据调查数据显示，2023 年，82.42%的用户倾向于使用一体化的云原生应用保护平台，仅有 17.58%的用户表示希望在各个阶段分别使用独立的安全工具。

图 17 用户云原生安全建设模式选择

（四）云原生安全关键能力剖析

集群配置错误成为用户最关注的 kubernetes 安全风险之一。针对集群资源的攻击、集群组件漏洞，以及集群配置错误成为用户最关注的 kubernetes 安全风险前三名，其关注度分别为 48.01%、47.7%、41.22%。另外，27.98%的用户关注 kubernetes 集群的权限分配不当，26.43%的用户关注 kubernetes 运行时攻击安全风险，18.39%的用户关注 kubernetes 的网络风险。

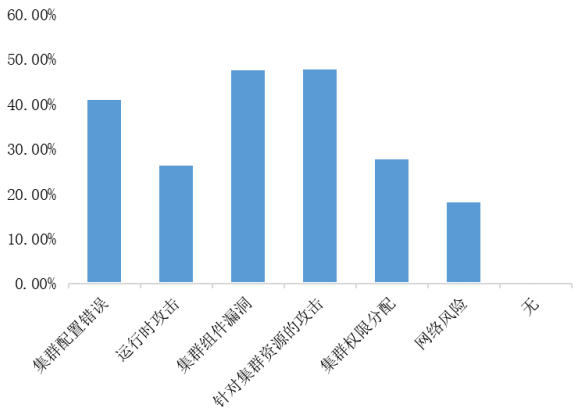

图 18 kubernetes 安全风险关注度

特权容器启动、容器敏感挂载、Kubernetes 未授权访问成为用户重点关注的云原生配置风险。云原生配置风险方面，容器敏感挂载成为用户最关注的风险，占比 59.3%，特权容器启动紧随其后占比 58.28%，用户对 kubernetes 未授权访问的关注度有所提升，占比 43.89%。另外，有 32.7%的用户选择了容器使用未限制内存，仅有 14.82%的用户选择了非受信镜像使用。

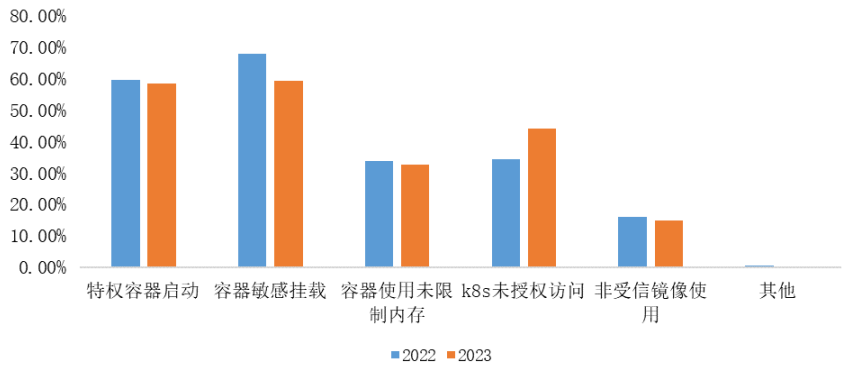

图 19 用户最关心的云原生配置风险

恶意访问、恶意命令执行仍是用户最关心的容器运行时安全问题。在用户最关心的容器安全问题方面，超六成用户依旧最关注恶意访问和恶意命令执行两类容器安全问题，其关注度分别占比 65.19%和 60.09%。其他容器安全问题中，恶意命令持久化占比 56%，权限提升占比 37.09%。防护绕过、凭据访问、网络探测的占比有所提升，分别占比 41.73%、26.74%、23.18%，其他容器安全问题占比不足两成。

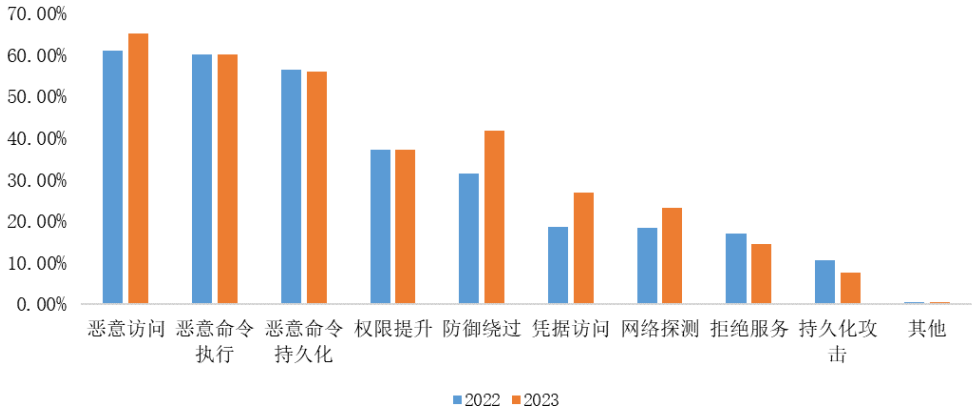

图 20 用户最关心的容器运行时安全问题

用户最关心的云原生应用安全问题前三分别是 API 滥用、DDoS 攻击、未授权访问。在用户最关心的云原生应用安全方面，仍然有超半数用户最关心 API 滥用、DDoS 攻击、未授权访问问题，分别占比 57.97%、62.41%、61.11%。应用漏洞、密钥管理不规范，以及应用间通信加密的关注度显著提升，分别占比 40.96%、38.79%、30.91%，访问权限配置错误占比依然不足一成（8.68%）。

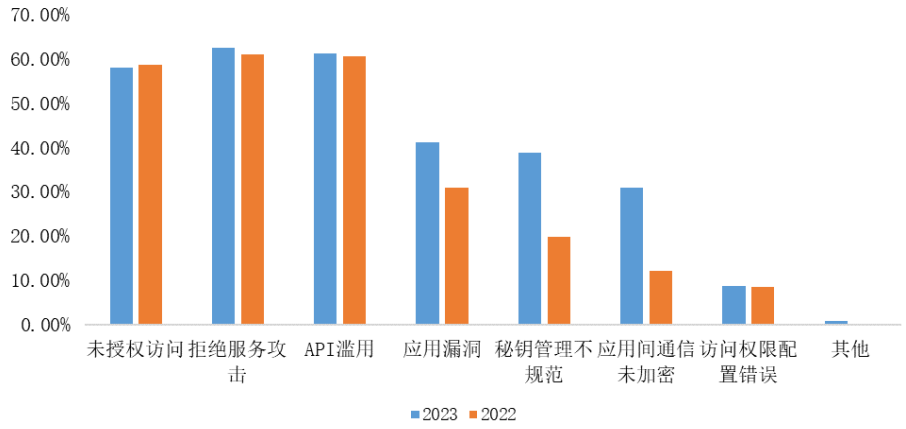

图 21 用户最关心的云原生应用安全问题

云原生基础设施配置的风险检测是用户对云安全运营的基本需求。在云原生环境下，42.66%的用户表示云上安全运营需要做好云原生基础设施配置的风险检测。另外，34.05%的用户希望云上安全运营具备多云、混合云环境下安全态势的统一管理。30.96%的用户认为在云原生环境下，攻击面进一步扩大。用户也需要云上安全运营可以进行弹性动态的资产管理手段、简单化云上安全合规管理、增强自动化相应处置机制与能力，这部分用户占比分别为 22.87%、27.36%、24.47%。初次之外，也有 7.73%的用户认为云上安全运营需要进行相关人才培养、培训措施。

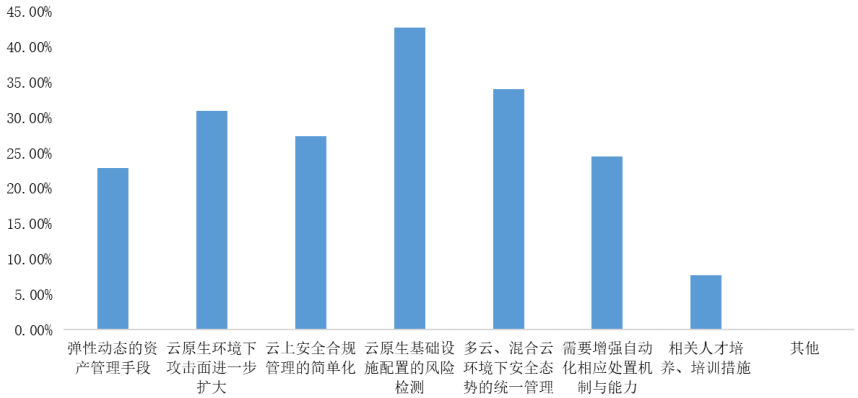

图 22 云原生环境下安全运营面临的需求

基线扫描工具成为保障云原生安全的重要工具，超 9 成用户开展云原生安全基线工具建设。通过云原生安全基线扫描，企业可以及时发现并解决安全问题，提高云原生应用的安全性和稳定性，保障企业数字化转型的顺利进行，因此越来越多的企业开始建设云原生安全

基线扫描工具。据调查数据显示，已有 59.51%的用户已经具备云原生基线扫描工具，31.92%的用户计划建设云原生全基线扫描工具，仅有 7.57%的用户不计划建设云原生安全基线扫描工具。

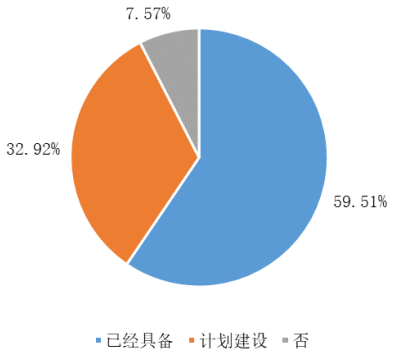

图 23 用户云原生安全基线工具建设情况

国内云原生基线规范发展仍处于相对初级阶段。现阶段，国内各企业大多遵循 CIS 相关标准，CIS 标准范围有限并不符合国内应用场景的实际要求，因此国内亟需发展云原生相关基线规范。2023 年，中国信通院牵头组织行业专家共同编写并发布了《云原生安全配置基线规范》v1.0。当前 57.21%的用户依然使用 CIS 规范，41.76%的用户使用内部设计规范，仅有 1.03%的用户使用国内的基线规范标准。但是数据显示，未来有 57.24%的用户计划使用国内标准为内部安全基线规范 32.57%计划使用自主设计规范，10.19%的用户计划采用 CIS 规范。

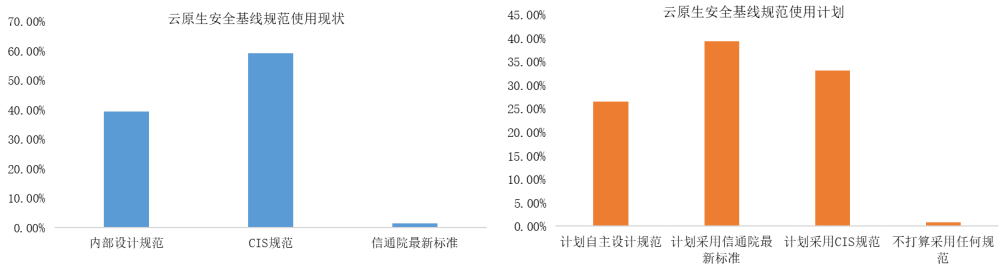

图 24 云原生安全基线规范用户使用现状与计划

云原生安全验证手段多样化发展，已有 20%的用户开始使用自动化的攻击模拟工具。安全验证是云安全运营的重要技术之一，例如红蓝对抗、渗透测试等，都是企业用来检验安

全能力有效性的常用方案。在云原生安全能力验证手段选择方面，据调查数据显示，51.78%的用户使用漏洞扫描，46.58%的用户使用渗透测试，38.44%的用户使用红蓝对抗，20.37%的用户使用针对云原生安全入侵与攻击模拟（CNBAS）工具进行安全验证。

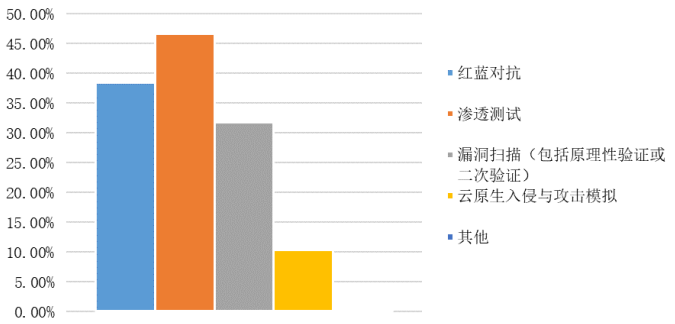

图 25 云原生环境下的安全验证手段

缺乏测试标准成为用户云原生安全验证的最大难题。在云原生环境下，43.62%的用户认为没有可依据的测试标准是安全验证面临的最大难题，40.06%的用户表示现有安全验证手段覆盖面窄，32.17%、31.74%的用户则认为现有安全验证手段无法适用于云原生安全环境、无法保证验证结果的一致性和可靠性，24.05%、24.35%的用户认为效果不佳和耗时过长是云原生安全验证面临的最大难题，有不足两成的用户认为现有安全验证手段成本过高。

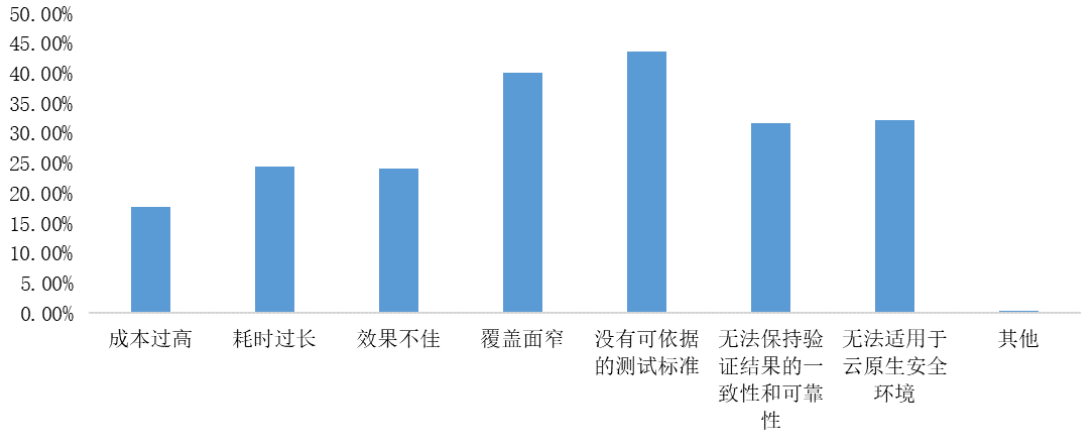

图 26 云原生环境下安全验证的最大难题

云原生入侵与攻击模拟（CNBAS）技术受到关注度，约 40%的用户计划试用 CNBAS 工具。云原生弹性扩展、灵活部署的特性使得云上环境更加复杂多变，传统 BAS 技术很难对云原生环境做到全面、精细的攻击模拟，因此，CNBAS 作为针对云原生环境进行入侵和

攻击模拟的安全验证技术，受到了云原生安全用户的关注。据调查数据显示，58.03%的用户表示暂时不考虑试用 CNBAS，15.66%的用户表示会在测试环境中试用 CNBAS，13.65%的用户表示会在灰度环境中试用CNBAS，12.66%的用户表示会在生产环境中试用CNBAS。

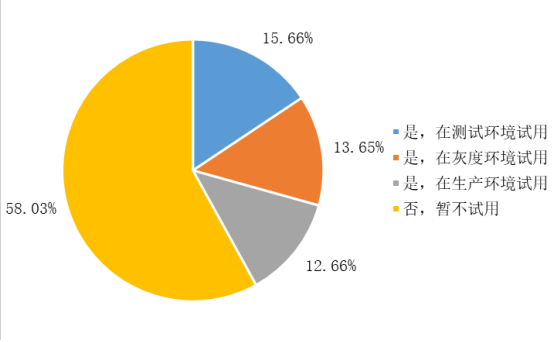

图 27 云原生入侵与攻击模拟（CNBAS）的采纳率

云安全托管服务（MSS）价值认同逐步提升，公有云上业务已开始享受便利。对于中、小企业来说，基于云原生的安全运营建设又面临着技术复杂、成本高昂的诸多问题，因此，使用公有云安全产品辅助自主运营成为更多企业的选择。调查显示，47.34%的用户使用公有云安全产品辅助自主运营，40.36%的用户自主建设自主运营，15.3%的用户使用安全厂商提供的云安全托管服务。

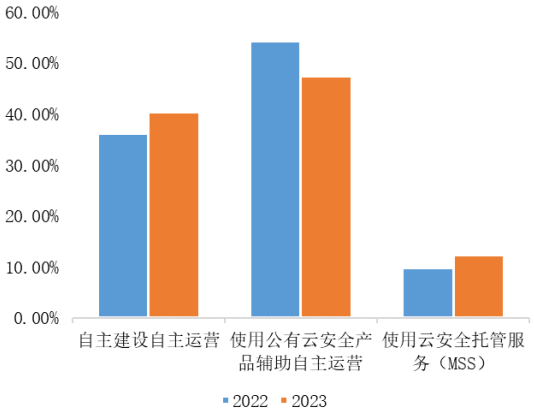

图 28 云原生安全运营模式采纳情况

便捷、专业和降本是用户选择云安全托管服务的主要原因。数字化转型浪潮下，众多新兴技术快速发展，云安全托管服务以其方便、快捷、高效、专业的优势开始被众多用户认可。调查显示，40.36%的用户看重云安全托管服务的便捷性，25.45%的用户因其具有专业的安

全服务团队，安全防护能力更强而选择 MSS，20.45%的用户因其可以降低安全服务成本，16.31%的用户需要第三方服务团队帮助测评评估安全体系而选择 MSS，另有 1.43%的用户是为了体验新服务理念。

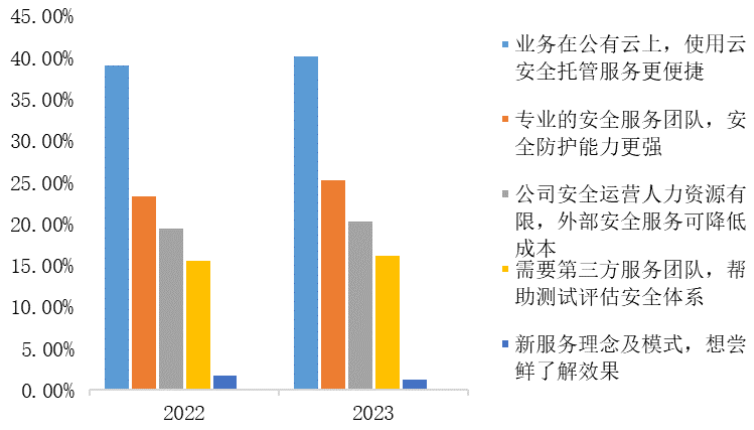

图 29 用户选择托管服务的主要原因

四、云原生安全建设趋势

人工智能未来或将引发云原生安全领域新变革。近几年，伴随着大模型的异军突起，人工智能技术再度引发全球范围内的高度关注，AI 技术在各领域重焕新机，也带来了云原生安全领域新一轮的潜在机遇。据调查数据显示，31.07%的用户非常关注人工智能在云原生安全领域的应用，33.23%的用户一般关注，25.4%的用户有一点关注，仅有 10.3%的用户表示完全不关注人工智能在云原生安全领域的应用。

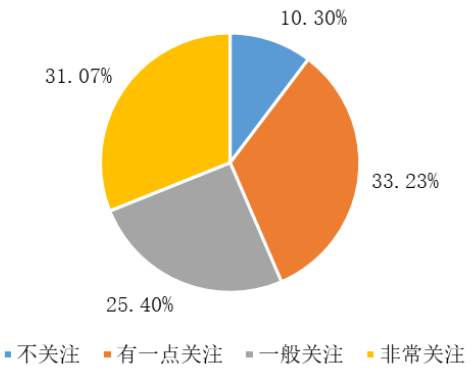

图 30 用户对人工智能的关注度

80%以上用户认为未来云原生安全将朝着原生化、一体化、智能化不断演进。60.12%的用户未来会推动安全服务云原生化，使安全服务更加敏捷灵活；50.19%的用户未来会建设适配多云环境的一体化安全平台；40.12%的用户未来会增强智能化安全防护，将 AI 技术融入安全防护全流程；仅有 24.84%的用户未来计划借鉴 CNAPP 安全框架，补足自身安全短板。

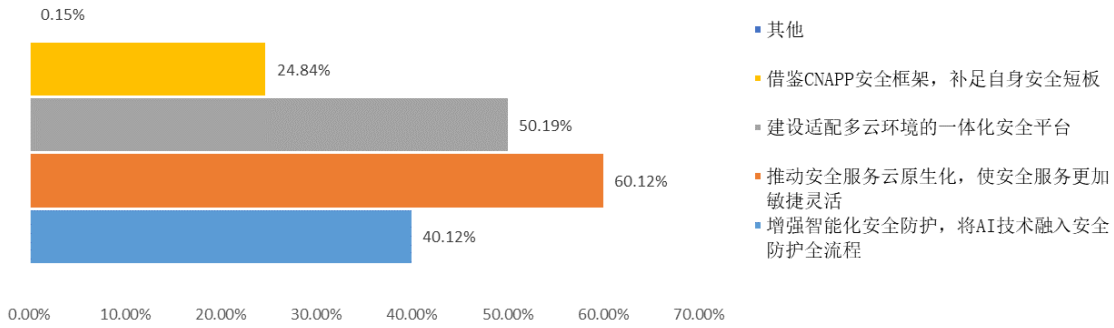

图 31 用户计划发展的云原生安全新方向