云原生应用保护平台 (CNAPP) 调查报告

Microsoft

CSA GCR cloud security GREATER CHINA REGION alliance®

CSA cloud security alliance®

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网（https://c-csa.cn）

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《云原生应用保护平台（CNAPP)调查报告（CNAPP Survey - Sponsored by Microsoft）》由CSA工作组家编写，CSA大中华区秘书处组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组长：刘文懋

翻译组：

白玉强　　崔崟　　伏伟任　　李卓嘉　　廖武锋　　鹿淑煜

申屠鹏会

研究协调员：

卜宋博

感谢以下单位的支持与贡献：

北京神州绿盟科技有限公司　　北京沃东天骏信息技术有限公司

奇安信网神信息技术（北京）股份有限公司　　三未信安科技股份有限公司

上海物盾信息科技有限公司　　中国工商银行股份有限公司

感谢我们的赞助商

云安全联盟（CSA）是一个由会员驱动的非营利组织，致力于定义和提高对最佳实践的认识，以确保安全的云计算环境。CSA 利用行业从业者、协会、政府及其企业和个人成员的专业知识，提供云安全相关的研究、教育、认证、活动和产品。CSA 的活动、知识和广泛的网络使受云影响的整个社区受益，从供应商和客户到政府、企业家和保险行业，并提供一个多方共同合作的平台，以创建和维护一个可信的云生态系统。CSA 研究以供应商的中立性、敏捷性和结果的完整性而自豪。

感谢我们的赞助商微软（Microsoft）为研究的开发提供资金支持，并通过 CSA 研究生命周期的确保质量控制。赞助者是支持研究项目结果的 CSA 公司会员，但对 CSA 研究的内容开发或编辑权没有额外的影响。

关于赞助商

微软安全帮助保护人员和数据免受网络威胁，让您安心。

欲了解更多信息，请访问：https://www.microsoft.com/en-us/security

英文版本编写专家

主要作者：

Hillary Baron

贡献者：

Marina Bregkou　　Josh Buker　　Ryan Gifford

Sean Heide　　Alex Kaluza　　John Yeoh

设计师：

Claire Lehnert

特别感谢：

Adwait Joshi　　Thomas Zou

在此感谢以上专家。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给予雅正！ 联系邮箱research@c-csa.cn； 国际云安全联盟CSA公众号。

序言

在这个日益全球化的数字时代，云计算作为技术革新的核心，正不断推动着企业的数字化转型。作为这一领域的先锋，《云原生应用保护平台（CNAPP）调查报告》为我们提供了对云安全前沿的深刻洞察。得益于微软的赞助和 CSA 大中华区专家团队的卓越工作，本报告不仅仅是一个研究成果，更是一个全球视野下的指南。

报告详细探讨了云原生应用保护平台（CNAPP）在安全态势管理、云工作负载保护等方面的应用，强调了在 DevSecOps 实践中整合安全性的必要性。我们深入分析了自动化在提高云安全效率中的关键角色，以及如何在灵活性和响应能力保障的同时维护安全。报告中还阐释了面对不断演变的安全威胁，企业如何有效实施云安全策略，以及如何应对数字化转型过程中出现的新挑战。

本报告的核心在于它不仅为全球范围内的企业和技术专家提供了宝贵的见解，还为整个云安全社区搭建了一个交流和合作的平台。我们希望它能激发更多的行业讨论，推动更广泛的合作与创新，共同构筑一个更安全、更高效的数字世界。

在数字化和云计算不断发展的今天，这份报告不仅是云安全领域的重要参考，也是每一位致力于数字化转型的专业人士的必读之作。让我们一起探索云计算的未来，共同应对挑战，迈向更加安全、智能的数字化新时代。

李雨航 Yale Li

CSA 大中华区主席兼研究院长

目录

调查的创立和方法论

云安全联盟（CSA）是一个非营利组织,其使命是广泛推广确保云计算和 IT 技术中的网络安全最佳实践。CSA 还就所有其他形式的计算中的安全问题向这些行业的各个利益相关者进行教育。CSA 的会员包括行业从业者、企业和专业协会的广泛联盟。CSA 的主要目标之一是进行调查,评估信息安全趋势。这些调查提供了关于组织当前的成熟度、意见、兴趣和有关信息安全和技术的意图的信息。

微软委托了 CSA 开展一项调查和报告,以更好地了解行业对云原生应用程序保护平台（CNAPP）的知识、态度和观点。微软为该项目提供了资金支持,并与 CSA 研究分析师共同制定了调查问卷。该调查由 CSA 于 2023 年 4 月在线进行,收到了来自各种规模和地点的组织中的 IT 和安全专业人员的 1201 份回复。CSA 的研究分析师对本报告进行了数据分析和解释工作。

研究目标

调查的主要目标是更深入地了解以下内容:

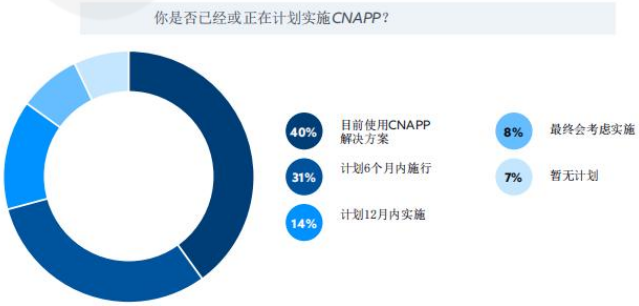
- 组织在云安全方面的优先事项和挑战
- 行业对 CNAPP 的熟悉程度和采用成熟度
- 安全态势管理、云工作负载保护和 DevSecOps（开发、安全和运营）的当前方法及挑战

关键发现

随着组织越来越多地利用多云策略,传统的安全解决方案通常很难为这些动态和分布式应用程序提供充分的保护。近年来，由于全面保护多云环境的复杂性以及整合组织当前部署的许多安全工具的能力，云原生应用保护平台已成为关键的安全工具类别，其中包括云安全态势管理（CSPM）、云工作负载保护（CWP）、云基础设施权限管理（CIEM）、网络安全和安全 DevOps。这项调查旨在了解组织在有效实施 CNAPP 方面的采用率和面临的挑战。 它旨在提供有关 CNAPP 部署的当前状态的见解,识别需要支持的领域,并指导决策制定。 以下是一些关键发现。

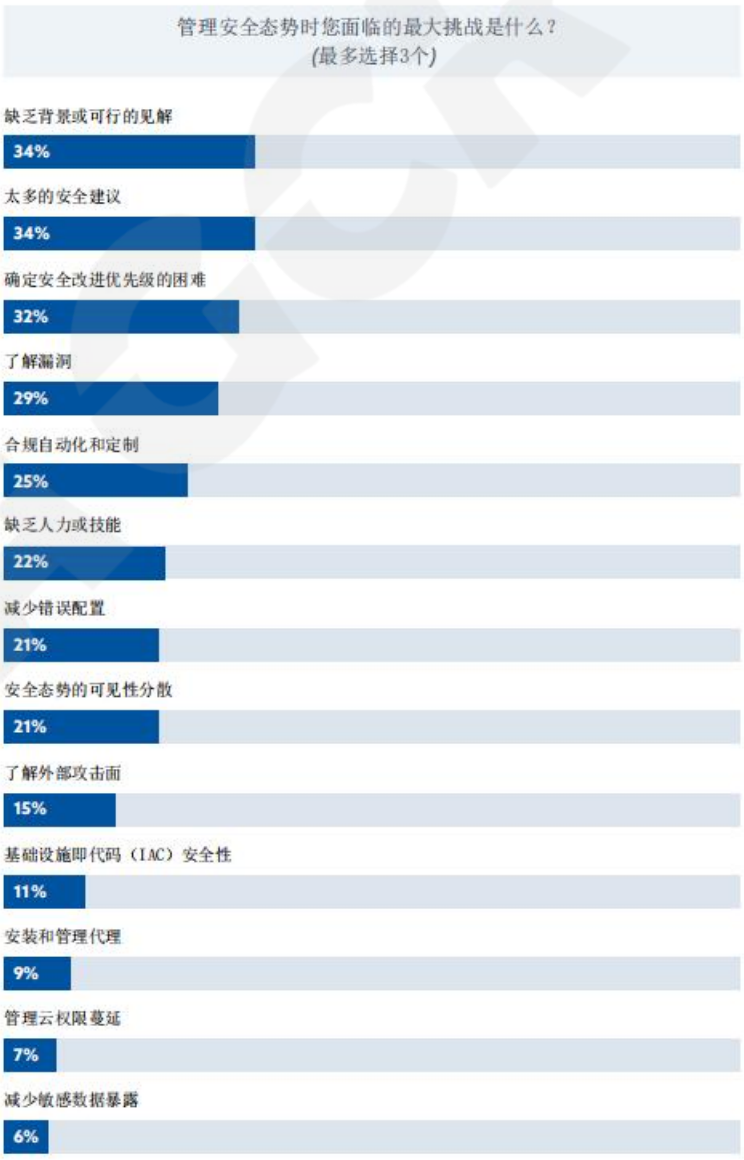
云原生应用程序保护平台:四分之三的组织选择使用 CNAPP来保护其多云环境

大多数组织(75%)已经或计划在其云环境中实施 CNAPP。 这一高采用率可以归因于多云策略的盛行，有 84%的组织使用了两个或多个云环境。 然而，现有的安全工具通常不足以充分支持如此复杂的多云设置，导致组织寻求像 CNAPP 这样的替代解决方案。 调查显示，仅有不超过 30%的组织通常将部署的安全工具（如 CSPM、CWP 和 CIEM）集成到多个云环境中。 在 CNAPP 提供的功能中，CSPM 凭借其在解决安全态势可见性方面的重要性成为关键吸引因素(25%)， 这被认为是组织的首要任务(42%)。这些数据清楚地说明了 CNAPP 为什么在组织中引发了广泛的兴趣。



云安全态势管理：安全团队需要明确的信息以进行适当的优先级排序

由于安全团队受到巨大数量警报的影响，他们在优化安全过程中一直在面临管理和优先级排序的困难。32% 的受访者透露，由于他们收到的信息数量庞大且经常不准确，他们在优先处理安全改进方面感到困难。 此外，34% 的人发现自己被安全建议所困扰，而同等比例的人缺乏相关或可操作的见解来做出明智的决策。 他们可能会收到大量警报或建议，但这些信息未能提供必要的详细信息以指导他们采取正确的行动方向。



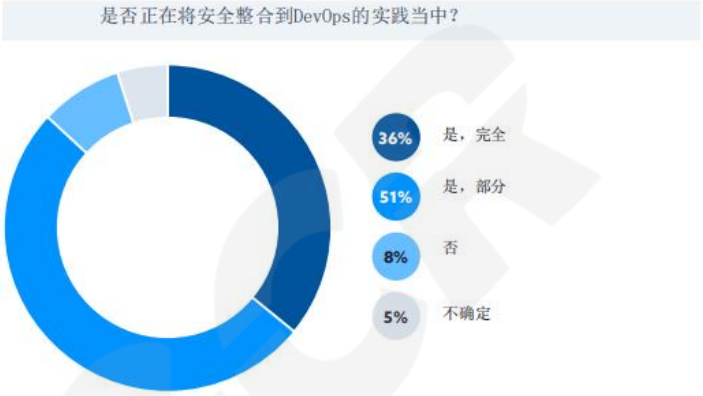
信息管理的问题与调查的另一个关键发现相关，即不同组织之间的监控设置存在广泛差异。有趣的是，33% 的受访者使用完全基于代理的监控系统，而 37% 的受访者则主要采用无代理方法，尽管他们还是会辅以一些基于代理的监控。 这种差异很可能受到特定供应商和组织可以访问的技术类型的影响。

总的来说，组织可能需要找到能够通过自动化和集中式的安全工具和技术来支持其安全态势管理。自动化将有助于缓解在优先级和建议（最佳实践）间的一些混淆。集中式的安全工具和供应商将帮助合并警报并提供更好的上下文信息，从

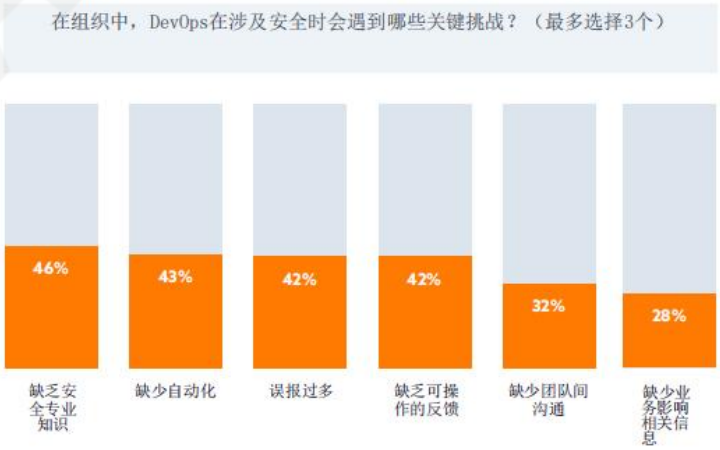
而帮助团队调整合适的优先级；最终帮助他们采取正确的行动。

DevOps 安全：DevOps 安全的重要性日益得到认可，但缺乏专业知识和人才阻碍了进程

尽管安全左移和 DevSecOps 是发展趋势，但是由于一些重大的问题阻碍了完全融合的进程，将稳健的安全措施整合入 DevOps 仍然处于早期阶段。目前，有 51%的组织正在将安全集成到他们的 DevOps 实践中，但只有 35%的组织声称已经完成了整合。其中的主要挑战在于：缺乏安全专业知识，自动化不足，过多的误报以及缺乏可操作的反馈。组织必须直面并解决这些问题以实现成功的整合。



在这些障碍中，首要的问题是缺乏安全专业知识，有46%的受访者报告了这一问题。这种不足可能会在 DevOps 的流程中引入漏洞，攻击者可能会潜在地利用这些漏洞。更麻烦的在于关于 DevOps 安全的责任和问责制存在模糊不清，不同的团队经常假设这是对方的责任。为了解决这个问题，组织应该为 DevOps 团队提供安全培训，聘请安全专家，并在组织内打造“安全为先”的文化。

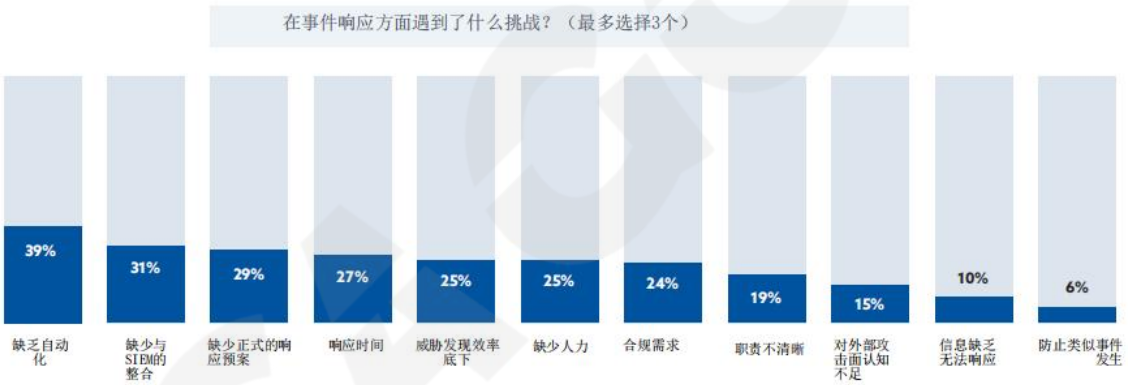


其它主要挑战都与技术相关，这其中最大的挑战是缺乏自动化，由43%的

受访者指出。缺乏自动化流程会使组织难以有效地管理和展开DevOps的落地。误报也是另一个重要的问题，有42%的组织被误报困扰。高误报率使得安全团队疲于应付，效率低下。最后，有42%的组织报告了缺乏可操作的反馈，这阻碍了他们对安全实践的有效响应。

与在安全态势管理上面临的挑战类似，教育、培训以及工具的质量是成功实现安全集成的要素。组织必须密切关注这些方面，以确保安全与DevOps的有效集成，从而更有效地保护其运营。

云工作负载保护：围绕事件响应的挑战回归为人员、流程和技术



在DevOps中，人员和技术挑战一直是焦点，但在涉及云工作负载保护和事件响应方面，问题涉及到所有方面：人员、流程和技术。

- 人员：25%的受访者认为人力资源缺乏是一项重要挑战。人手短缺妨碍了组织有效应对安全事件的能力，而缺乏规范的响应方案则会加剧这个问题。确保安全团队能够获得全面的培训、必要的工具和资源，将帮助他们更高效地处理安全事件。

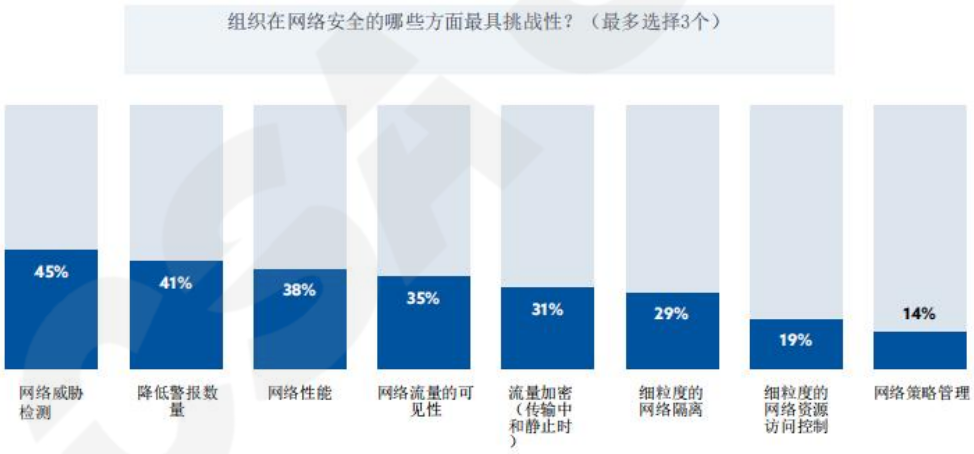
- 流程：29%的组织声称缺少正式的应急响应计划。没有清晰的路线图，组织往往难以理解他们在安全事件中的职责。为此，组织应当制定并实施正式的事件响应计划。该计划应当明确列出在面对安全事件时，事件响

应团队的职责和行动步骤。定期测试和更新响应计划以确保其有效性也至关重要。组织应积极发现并主动弥补事件响应计划中的潜在不足。

- 技术：缺乏自动化是组织正在努力解决的另一个关键挑战，有 39%的受访者报告了这一问题。自动化工具可以大幅减少响应时间，提高威胁调查的效率。因此，实施这些工具是改进事件响应的关键步骤。自动化事件响应流程的工具可以实时查看潜在的安全事件, 如 CNAPP 和安全信息和事件管理（SIEM）系统。组织还应在有助于评估安全事件优先级和减少误报数量的技术上有所投入，从而提高安全效率。

有效应对安全事件并保护云工作负载的能力源自人员、流程和技术。优先考虑这些领域将使组织能够强化其事件响应能力，从而确保其云工作负载得到坚实的保护。

网络安全：最成熟的实现，但威胁检测仍为挑战



在所有类别中，网络安全是最成熟的。值得关注的是，43%的受访者报告在多云环境中实现了网络安全的全面整合，而CSPM的整合率仅为28%。零信任战略的普及可能是这种成熟水平背后的一项关键驱动因素。然而，组织在网络安全方面仍然面临重要的挑战，在威胁检测和大量安全警报的管理方面尤甚。威胁的数量之多可能与组织环境的复杂性和大量网络流量有关。这种情况可能会使有效识别和跟踪潜在的安全威胁变得困难。

面对这些挑战，基于风险的方案将帮助组织优先关注更关键的资产和漏洞。这种方法确保首先解决高优先级的风险，从而强化组织的整体安全态势。此外，推荐充分利用支持多云环境并提供智能威胁防护的安全工具。如CNAPP之类的工具可以帮助自动化、简化并优化网络安全流程，有助于迅速识别和缓解威胁。

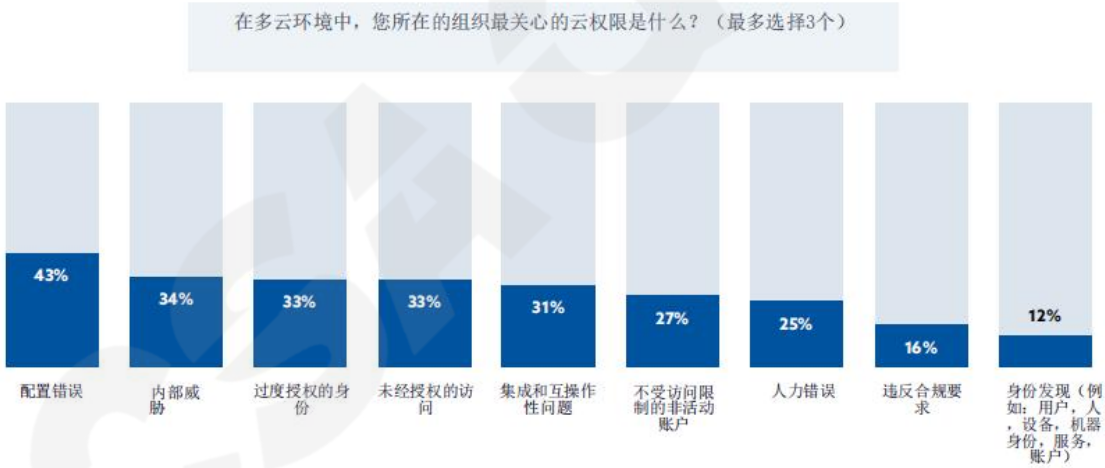
此外，减少安全警报的数量对于网络安全管理也很重要。一个可能的方向是对于能够有效区分真实威胁和误报的智能安全工具进行投入。这可以显著减少警报的数量，防止安全团队疲于应对，使他们能够集中精力应对真正的威胁。

尽管网络安全是多云环境涵盖的范围中最成熟的领域，但组织仍然面临重大挑战，特别是在威胁检测和安全警报管理方面。通过采用基于风险的方法，同时充分利用先进的安全工具，组织可以增强多云环境中的网络安全并且有效保护其资产。

云基础设施授权管理:高度关注权限配置错误

云基础设施授权管理（CIEM）遇到了一些显著的挑战，特别是在配置错误方面。近一半(43%)的组织认为他们最担心的问题是权限配置错误。这个普遍存在的问题可能会产生严重的后果，可能会导致未经授权的访问，甚至灾难性的数据丢失。错误的配置可能会在无意中暴露敏感数据或授予不必要的特权，从而创建可能被恶意行为者利用的漏洞。

为了解决这些问题，自动化安全工具越来越被认为是支持云基础设施授权管理（CIEM）的关键。这些工具可以对多云环境进行全方位扫描，允许对权限配置进行全面的观测和控制。这些工具通过主动检测和对配置错误告警，可以帮助组织快速解决问题，显著减少漏洞的窗口期。



结论

虽然CNAPP在几年前才被定义，但很快就被广泛接受了。许多企业目前正在使用或计划使用CNAPP。对于企业的吸引力在于能够提供全面的态势管理和可见性，以及为了降低风险而采用的代码上云的方法，这是企业最优先考虑的安全事项。CNAPP特别擅长保护多云环境，并为整合各种安全工具提供了统一的解决方案。

从调查结果中可以看出，企业面临的挑战往往围绕着两个核心因素：人员和技术。一方面，需要培养训练有素的专业安全人员，让他们清楚地了解自己的职责。另一方面，迫切需要有效的技术和工具来应对快速演变的网络安全威胁，并有效地支持安全团队。

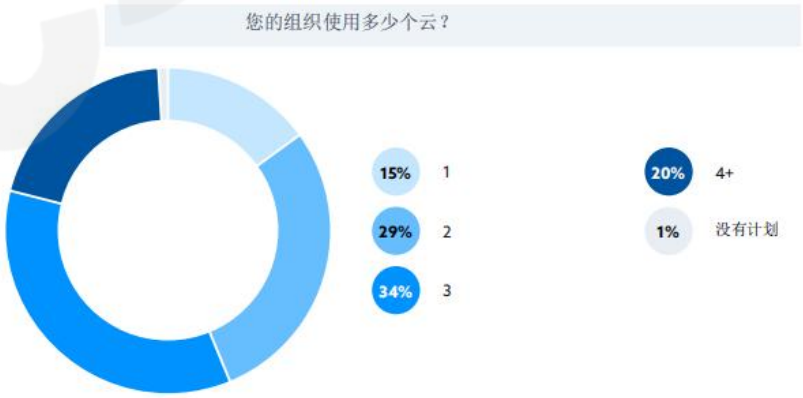
像CNAPP这类的技术必须能够为安全团队提供所需的正确信息和可见性，以便通过端到端实现平台治理的一致性，从而有效地保护多云环境。这种需求跨越了几个关键领域：云安全态势管理（CSPM）、云工作负载保护（CWP）、安全开发运维（DevSecOps）、云基础设施授权管理（CIEM）和网络安全。随着企业云上业务的发展，企业必须利用诸如CNAPP来为安全性提供集成解决方案，同时解决人员和技术方面的问题。这样，可以更好地为应对当今和未来的复杂网络安全挑战。

调研发现

云的使用和安全

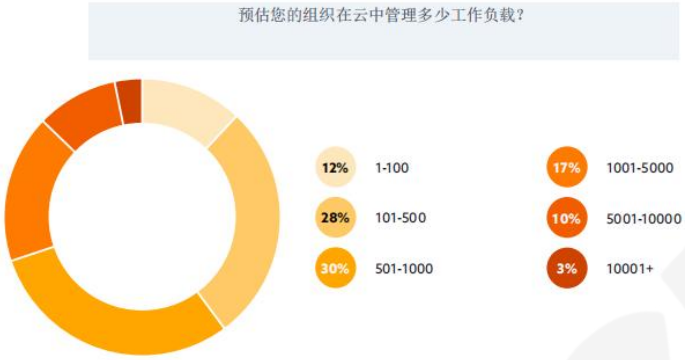
云环境

大多数组织都有两个或更多云的多云环境（84%）。只有15%使用单一云环境。



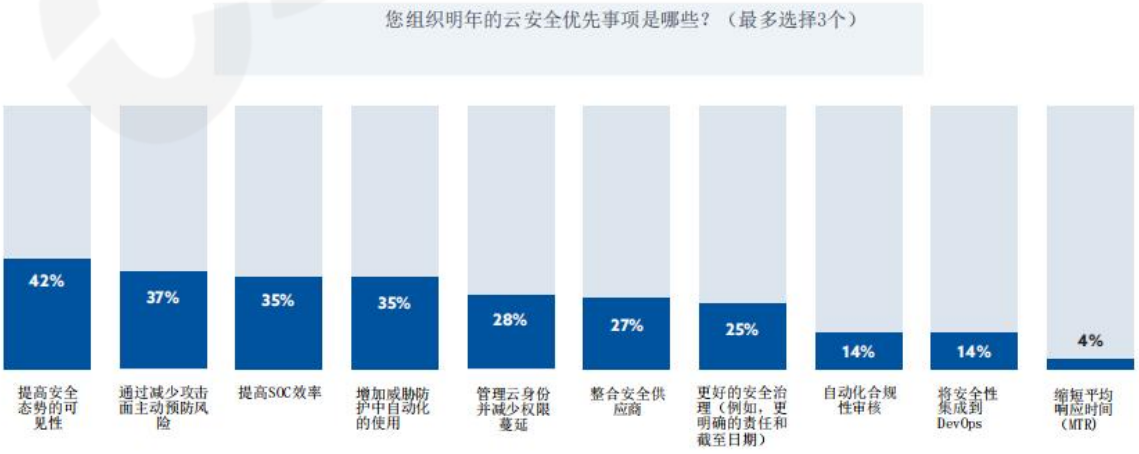
云中管理的工作负载数量

大多数组织在云中管理适量的工作负载。具体而言，28% 的受访者表示管理着 101-500 个工作负载，而 30% 的受访者表示管理着 501-1000 个工作负载。只有 3% 的组织报告工作负载超过 10,000 个。



今年安全工作重点

组织希望通过投资先进的安全工具和技术来改善其云安全状况。根据最近的一项调查，明年的三大优先事项是提高安全态势的可见性（42%的受访者）、增加威胁防护自动化的使用（35%）、提高 SOC （安全运营中心）效率（35%）以及通过减少攻击面来主动预防风险（37%）。这些优先事项表明，组织正在寻求更好地识别潜在漏洞，更快地检测和响应潜在威胁，并降低潜在安全漏洞的风险。

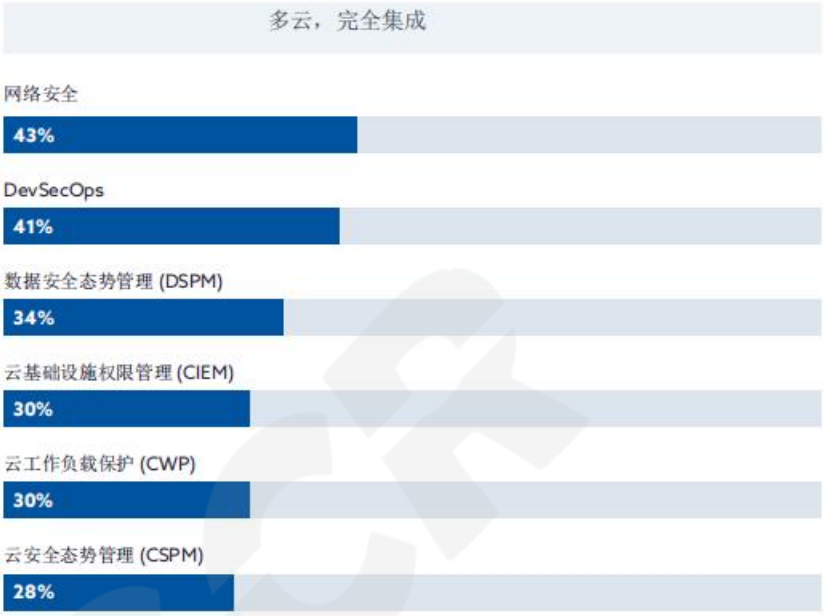


期望的安全结果

对于组织来说，最重要的安全成果是提高可见性，43% 的受访者选择将此作为首要任务。这表明组织正在寻求更好地了解其云安全状况，以识别潜在的漏洞并减少潜在安全漏洞的风险。第二个最重要的成果是减少手工工作，32% 的受访者选择了这一选项。这表明组织正在寻求自动化其安全流程，以提高效率并降低人为错误的风险。

跨多云环境的安全工具的成熟度

网络安全在多云环境中具有最高水平的完全集成，43%的受访者表示完全集成。DevSecOps 的完全集成程度位居第二，41% 的受访者报告跨多云环境的集成。CWP 和 CIEM 的集成程度相似，30% 的受访者表示两者完全集成。CSPM 和数据安全态势管理的完全集成程度最低，只有 28% 和 34%受访者分别报告了跨多云环境的集成。这些结果表明，组织在跨多个环境管理云安全时面临挑战，某些领域（例如网络安全和 DevSecOps）显示出更高级的集成。组织可能需要重新评估他们正在使用的安全工具，以确保其完整的多云环境受到保护和保障。

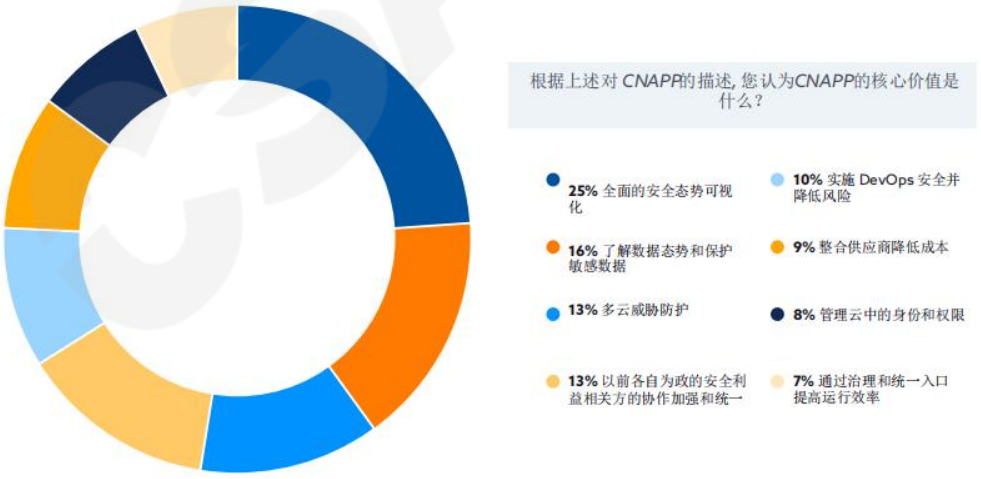


云原生应用保护熟悉云原生应用保护平台

大多数受访者（89%）都表示熟悉云原生保护平台（CNAPPs），只有11%的受访者表示不熟悉CNAPP。

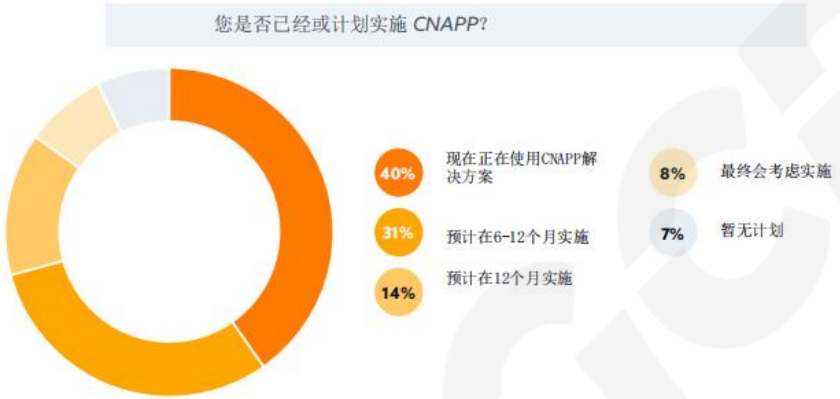
云原生应用保护平台的核心价值

受访者对云原生应用保护平台 （CNAPP） 的核心价值认识不一。选择最多的核心价值是获得全面的安全态势可视化，占受访者总数的 25%。其次，有 16% 的受访者选择了解数据态势和保护敏感数据作为核心价值。多云威胁保护，以前各自为政的安全利益相关方的协作加强和统一也被认为是重要的价值主张，选择这两项的受访者各有 13% 。



正在使用或计划使用CNAPP

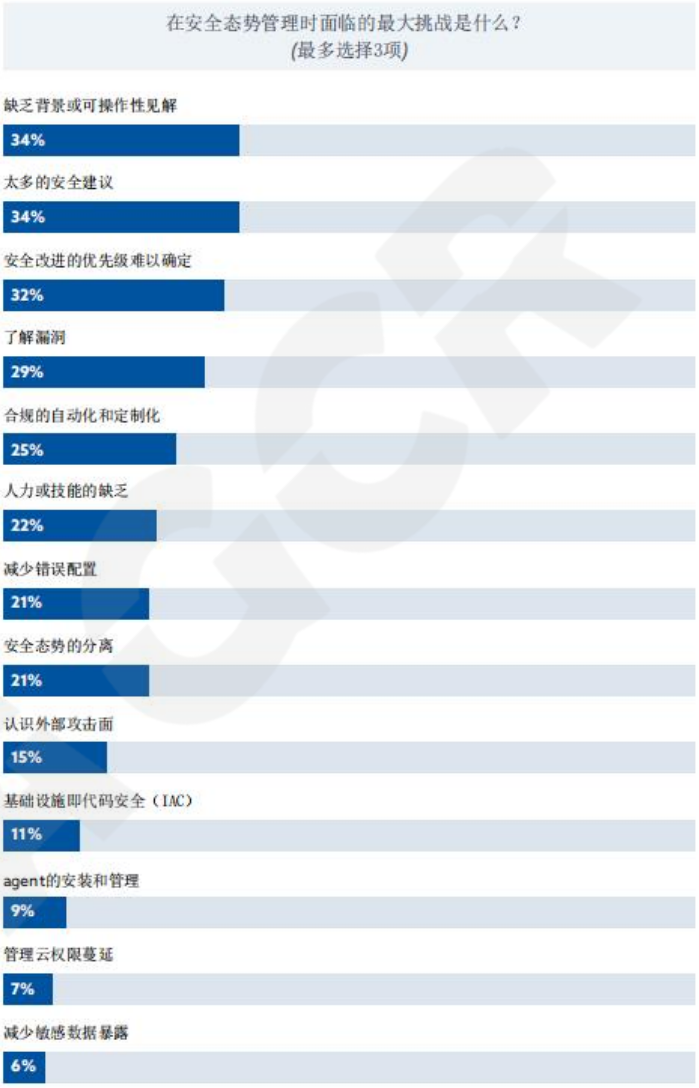
实施云原生应用保护平台(CNAPP)似乎是许多组织的首要任务，40%的受访者表示他们目前正在使用CNAPP解决方案。此外，31%的受访者表示计划在未来6个月内实施CNAPP，14%的受访者表示计划在未来12个月内实施CNAPP。只有8%的受访者表示有实施计划CNAPP但时间未定，剩下7%的受访者表示没有计划实施CNAPP。



云安全态势管理

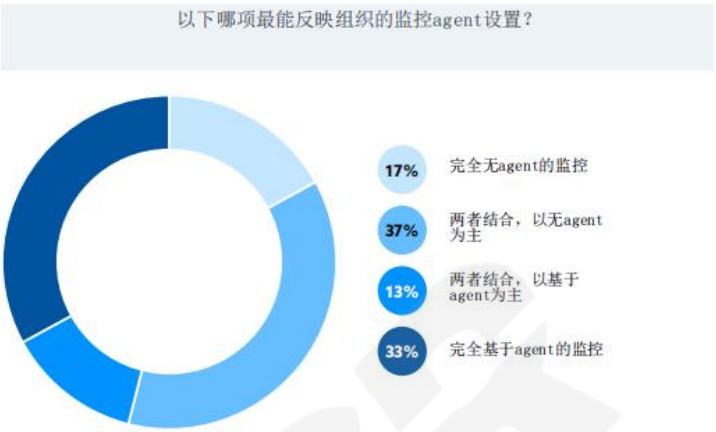
安全态势管理的最大挑战

企业面临安全态势的一些列挑战，其中背景或可操作性见解的缺乏和太多的安全建议是被选择最多的两项，分别有34%的受访者选择了这两项挑战。这表明企业正在努力获取正确的信息，以便对其安全状况做出明智的决策；同时也被大量无法提供清晰解决方案的建议所困扰。此外，有32%的受访者表示安全改进的优先级是一个重大的挑战。



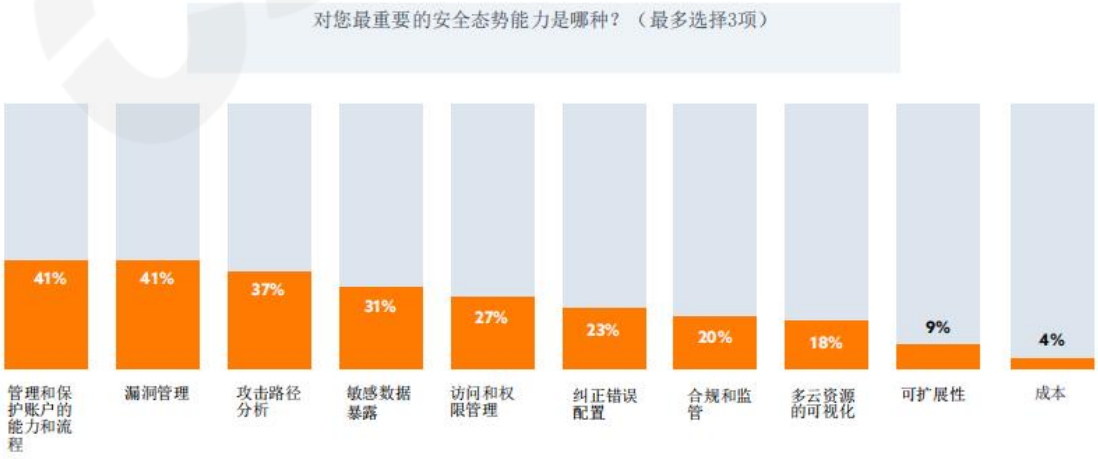
设置监控agent

调查结果表明，企业在设置监控的agent方面采取了不同的方法。17%的受访者报告使用完全无agent的监控，而33%的受访者报告使用完全基于agent的监控。更多的受访者（37%）表示组合使用两种监控方法，但以无agent的监控方式为主。还有13％的受访者表示使用两种监控方法的，但以基于agent的方法为主。这些结果表明，企业在监控环境时有不同的偏好和要求，可能需要根据具体需求或供应商来综合考虑各种方法。



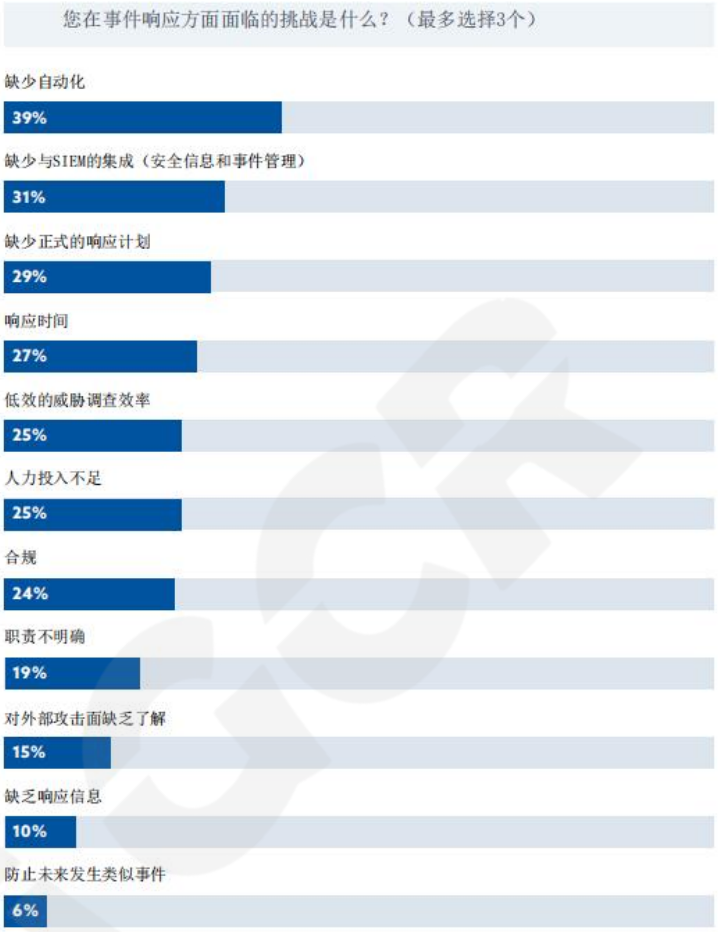
最重要的安全态势能力

管理和保护账户的能力和流程以及管理漏洞是被选择最多的两个能力，各有被41%的受访者选择。攻击路径分析也是一个高度受欢迎的能力，被37%的受访者选择。较少被选择为：敏感数据暴露（31%），访问和权限管理（27%）以及纠正错误配置（23%）。



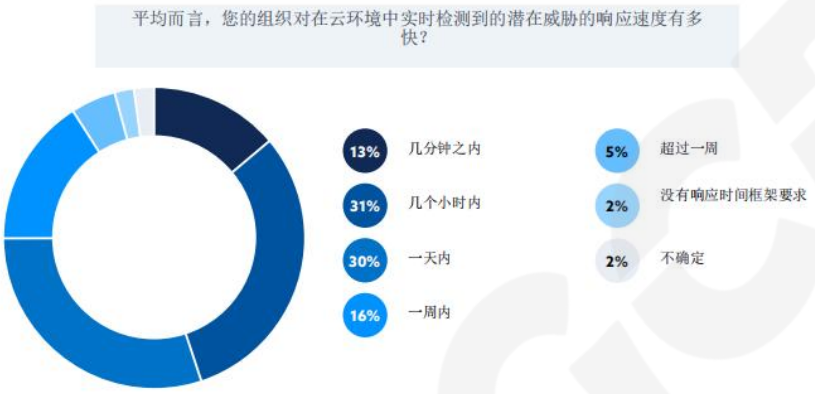
云工作负载保护事件响应的挑战

当涉及到事件响应时，组织面临着一系列挑战，技术缺陷是最受关注的问题。39%受访者选择了缺少自动化、31%选择了与SIEM的集成，29%选择了缺乏正式的响应计划。此外，27%的受访者提到了响应时间迟缓。值得注意的是，缺乏正式的响应计划会影响事件响应团队有效利用技术的能力，这对于任何有效的事件响应都是必要的。



检测到威胁后的平均响应时间

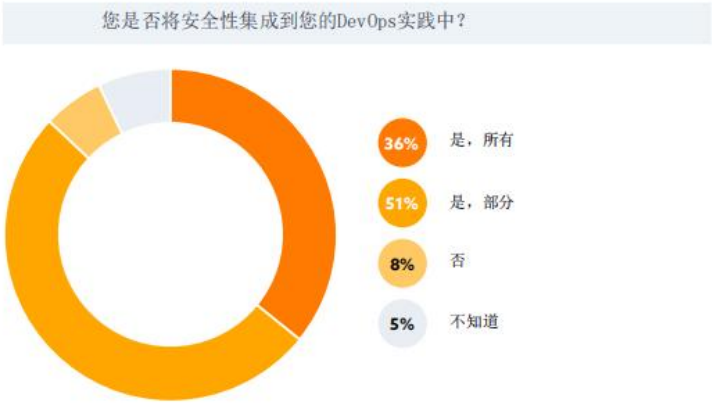
当涉及到在云环境中实时检测到的潜在威胁时，组织的响应时间不同。13%的受访者声称在几分钟内响应，31%在几小时内响应，30%在一天内响应。值得注意的是，几分钟内的响应时间可能需要供应商或自动化在事件响应过程中提供协助。另一方面，16%的受访者需要超过一周的时间来响应，只有2%的受访者没有设定响应的时间框架。



安全DevOps

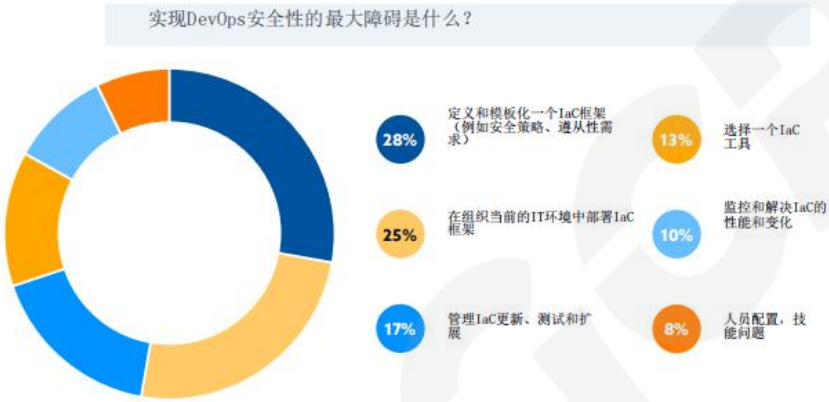
将安全性集成到DevOps实践中

大多数受访者（87%）报告说，他们的组织已经实施或部分实施了DevSecOps实践，只有8%尚未实施。这与在软件开发生命周期中进行安全左移并将安全性集成到开发过程中的趋势是一致的。这也反映了支持这些实践的工具和技术的日益增加的可用性。



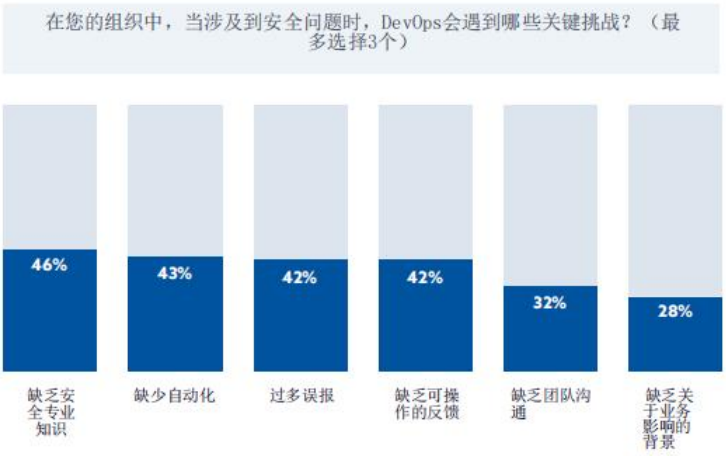
实现DevOps安全性的障碍

实现DevOps安全性的最大障碍似乎是出现在实施过程，最大的挑战集中在早期阶段。28%的受访者认为，定义和模板化IaC（基础设施即代码）框架，并包括安全策略和合规要求，是最大的障碍。紧随其后的是在组织当前的IT环境中部署IaC框架（25%）。管理IaC更新、测试和扩展（17%）以及选择IaC工具（13%）也被认为是障碍。人员配备和技能组合问题（8%）是最不常见的挑战。



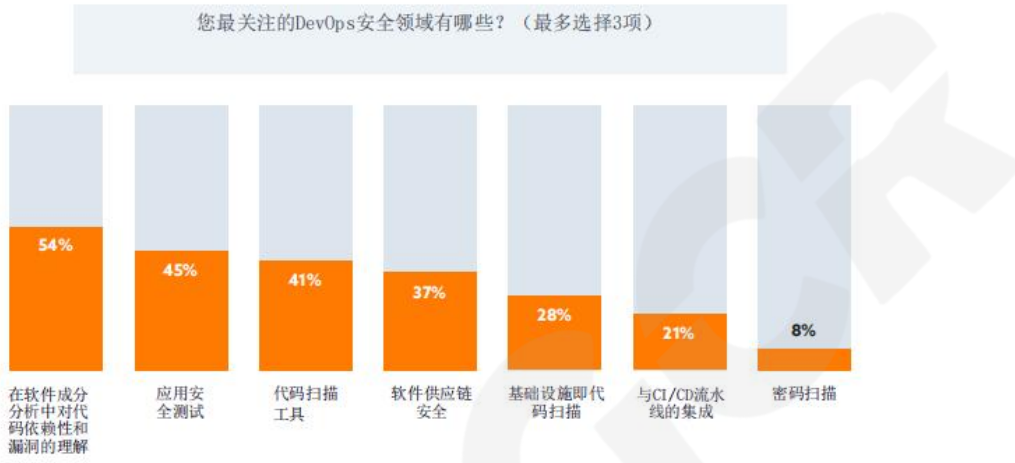
DevOps在安全性方面面临的主要挑战

当涉及到DevOps安全性时，组织面临着几个关键挑战。最大的挑战是缺乏安全专业知识，46%的受访者认为这是一个问题。缺少自动化是第二常见的挑战，占43%。太多的误报和缺乏可操作的反馈也构成了重大问题，42%的受访者认为这些都是挑战。其他常见的问题包括团队之间缺乏沟通和缺乏关于业务影响的上下文。解决这些挑战可以帮助组织更好地将安全性集成到他们的DevOps流程中，并确保他们的环境更加安全。



DevOps安全关注领域

DevOps安全主要关注领域包括：在软件成分分析中对代码依赖性和漏洞的理解（54%），应用安全测试（45%）以及代码扫描工具（41%）。其他重要的关注领域包括：软件供应链安全（37%），基础设施即代码扫描（28%），与现有CI/CD流水线的集成（21%），以及密码扫描（8%）。



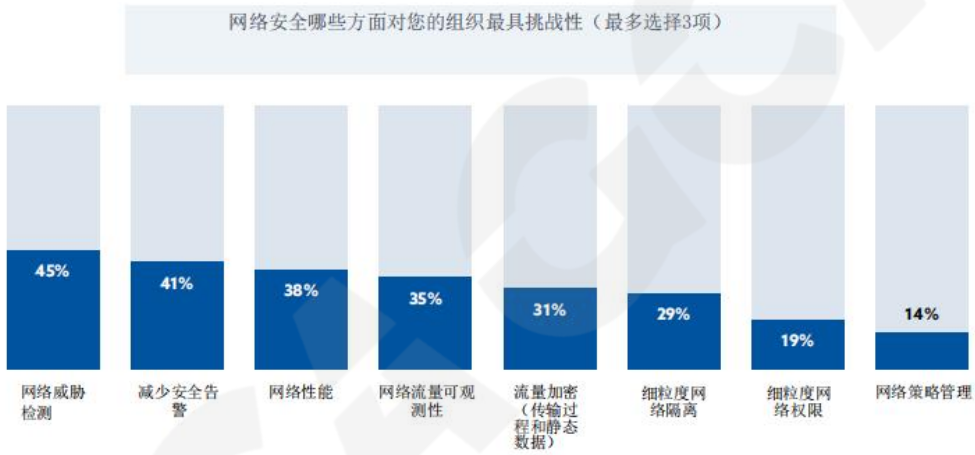
DevOps安全责任人

需要注意的是，由于调查对象主要是安全领域的从业人员，因此以下结果可能存在一定的偏差。当被问到在组织中谁负责DevOps安全时：20%的受访者回答是安全工程团队、17%回答是安全运维/管理团队、产品研发团队和风险管理团队各占12%。其他选项包括DevOps团队、首席信息安全官（CISO）办公室、系统管理员、质量保证（QA）/质量（QC）控制团队、云工程团队和特定的开发人员则回答较少。

网络安全和云上权限

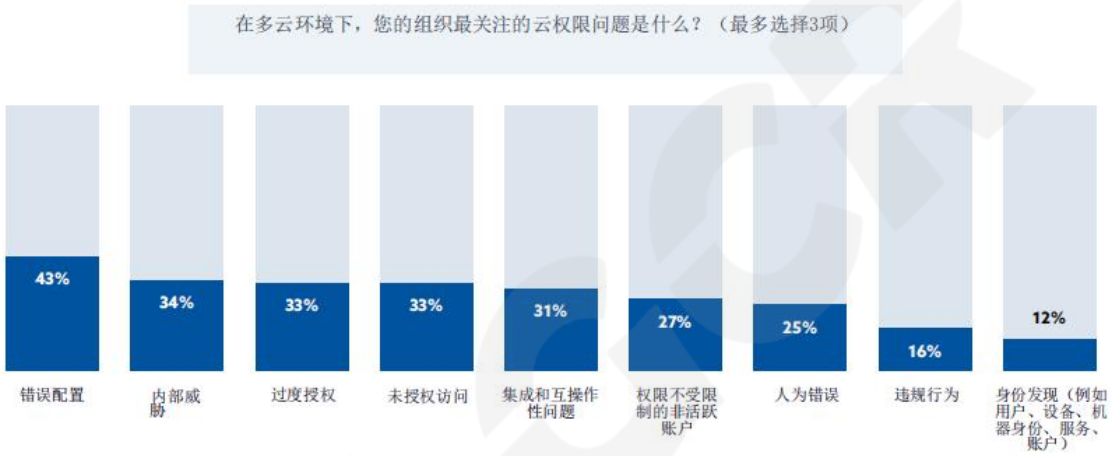
网络安全挑战

45%的受访者表示，网络威胁检测是网络安全中最具挑战性的方面，这表明在检测和响应潜在安全威胁方面存在困难。减少安全警报数量是第二个最具挑战性的方面，41%的受访者表示他们难以应对安全工具生成的大量警报。对网络流量的可观测性也是一个重要挑战，35%的受访者报告称他们难以完全了解自己的网络流量。其他网络安全方面，如细粒度的网络隔离、流量加密和网络策略管理，有较少的受访者选择。



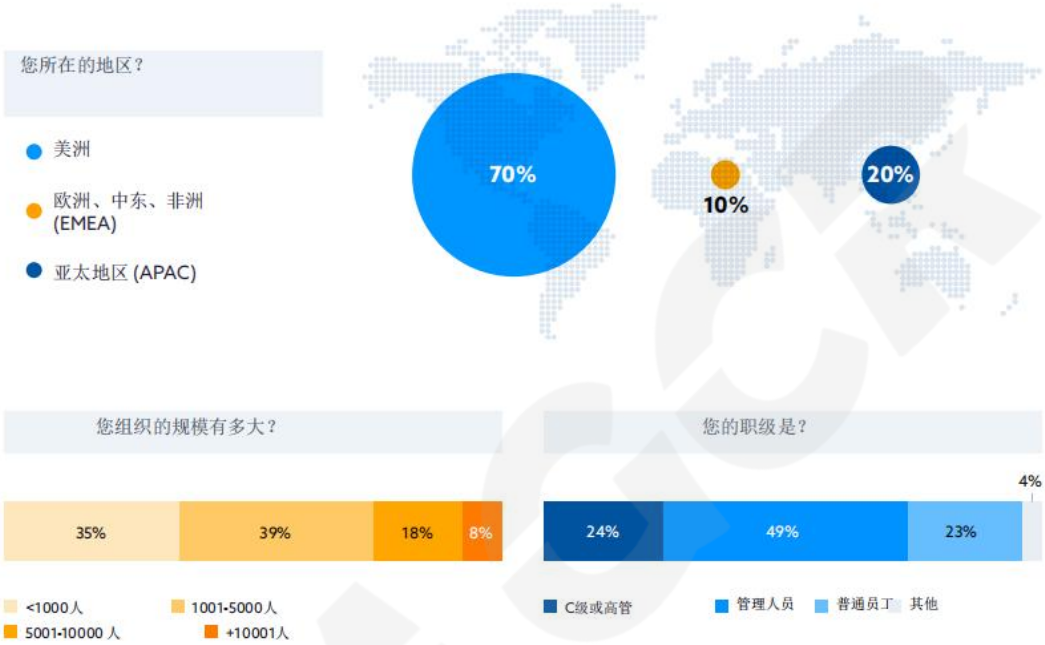
多云环境下的权限问题

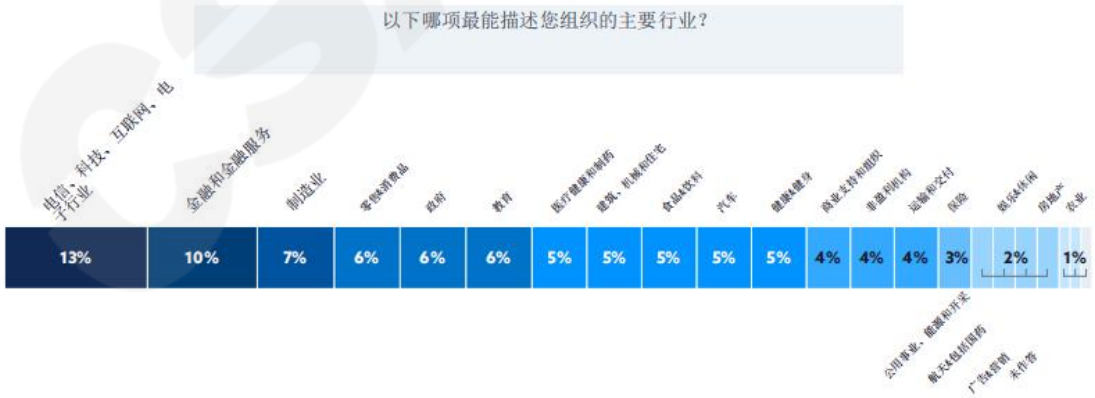
对于43%的受访者来说，在多云环境下云权限的错误配置是最令人担忧的问题。这表明组织在正确配置云权限方面存在困难，这可能导致潜在的安全漏洞和未授权的访问。内部威胁和权限过高的身份也是重要的关注点，分别有34%和33%的受访者将其选择为最重要的问题。其他问题，如具有无限制访问权限的非活动账户和集成问题，则被选择的频率较低。



统计来源

该调查由CSA于2023年4月在线进行，收到了来自不同规模、地域组织的IT和安全专业人员的1201份回复。





CSA GCR cloud security alliance
GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905