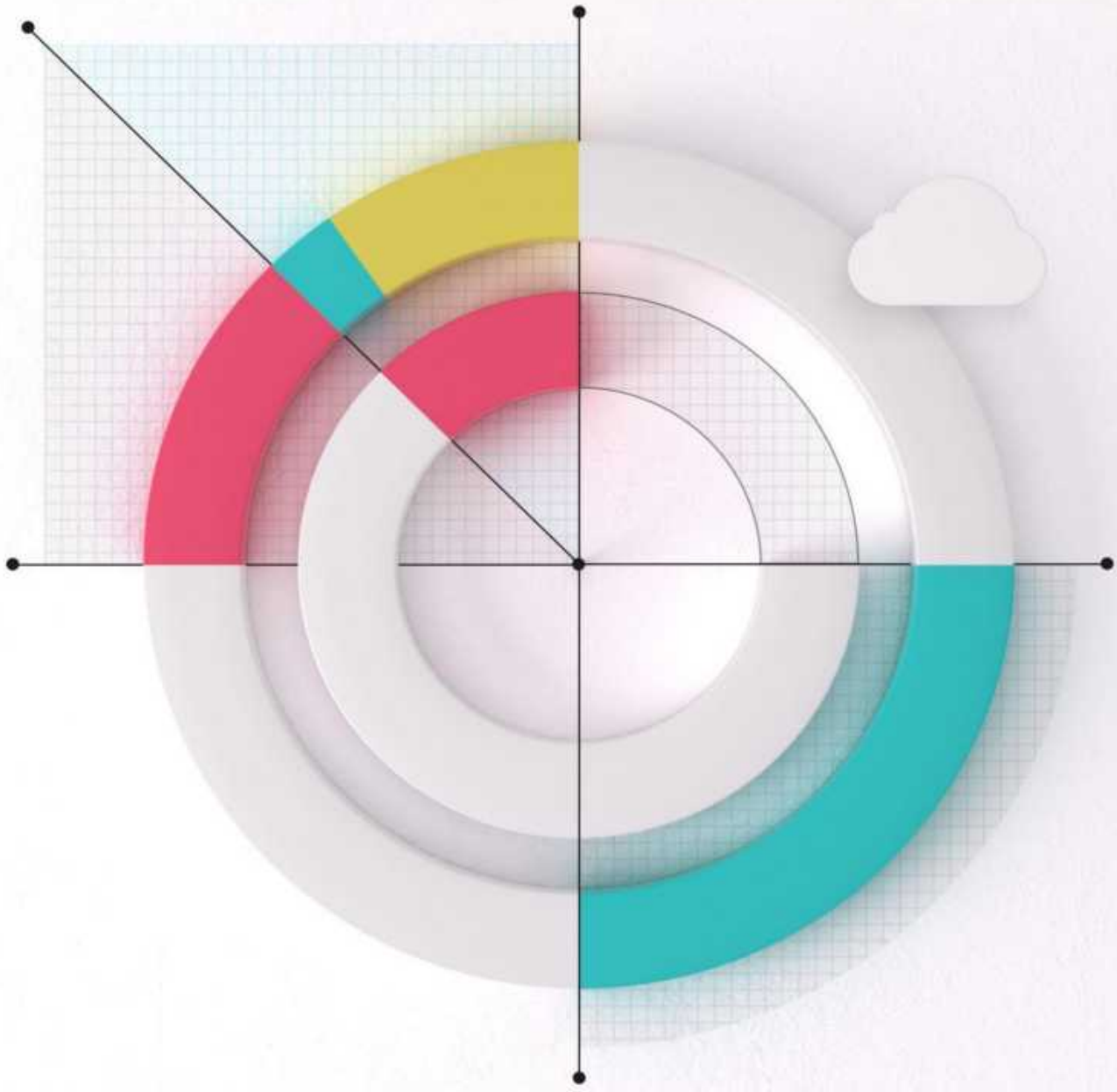
ADAPTIVE SHIELD

CSA GCR cloud security alliance GREATER CHINA REGION

CSA cloud security alliance

年度SaaS安全调查报告

2024计划和优先事项



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

《年度SaaS安全调查报告（SaaS Security Survey Report ）》由CSA工作组专家编写，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：

郭鹏程

翻译组：

曹莉　丁振涛　李清　李晓川　刘亚丽　陶瑞岩　于新宇

审校组：

郭鹏程

研究协调员：

闭俊林　梁嘉荣

感谢以下单位的支持与贡献：

北京金山云网络技术有限公司　杭州默安科技有限公司

上海安几科技有限公司　浙江大华技术股份有限公司

中国工商银行股份有限公司

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 秘书处给予改正！ 联系邮箱 research@c-csa.cn；国际云安全联盟 CSA 公众号。

英文版本编写专家

主要作者：

Hillary Baron

贡献者：

Josh Buker　Marina Bregkou　Ryan Gifford　Sean Heide　Alex Kaluza

John Yeoh

设计师：

StudioYael

特别感谢：

Hananel Livneh　Arye Zacks　Caroline Rosenberg　Eliana Vuijsje

序言

在数字化转型的浪潮中，软件即服务（SaaS）作为企业关键业务支撑和数据承载的重要平台，其安全性对于保障企业运营稳定与数据资产安全至关重要。随着SaaS应用的广泛普及和深度融入企业运作，针对SaaS环境的安全威胁与挑战也呈现出日益复杂且频繁的态势。在此背景下，《年度SaaS安全调查报告》应时而生，旨在全面剖析当前SaaS安全领域的现状，揭示行业面临的挑战与机遇，为全球组织提供关键洞见与行动指南。

本报告由云安全联盟（Cloud Security Alliance, CSA）的专业团队精心编制，汇集了全球范围内数百家组织的宝贵经验和实地调研数据。通过对SaaS安全事件、现有安全策略与方法、利益相关者角色、用户设备监控、投资趋势等方面的深度剖析，报告呈现了SaaS安全生态系统的全貌，为读者揭示以下关键发现：

SaaS安全事件呈上升趋势过去两年中，55%的组织经历了至少一次SaaS安全事件，表明针对SaaS的攻击行为正日益加剧。这促使企业必须清醒认识到，传统针对本地部署环境的威胁，如勒索软件、恶意软件和数据泄露，同样可能在SaaS环境中造成严重影响。现有SaaS安全策略与方法的局限性超过半数（58%）的受访组织认为其当前的SaaS安全解决方案仅覆盖了应用程序的一半或更少。人工审计与云访问安全代理（CASB）等常用工具在应对SaaS安全事件时暴露出局限性，呼唤更为先进且全面的防护手段。SaaS应用程序利益相关者范围分散随着SaaS所有权在组织内部的分散，CISO和安全管理者的角色转变为协调者，凸显了跨部门协作在确保SaaS全栈安全中的核心地位。SaaS安全投资显著增长大量组织显著增加了对SaaS应用程序及其安全工具的投资，其中SaaS安全态势管理（SSPM）解决方案的采用率在一年内由17%激增至44%，显示了企业对强化SaaS安全的迫切需求与坚定决心。对SaaS安全生态系统的全面关注企业愈发关注SaaS生态系统中的广泛问题，包括错误配置、跨SaaS访问、设备到SaaS的风险管理、身份与访问治理以及身份威胁检测与响应（ITDR），并致力于制定强有力的策略、流程和能力以应对这些领域的安全挑战。

《年度 SaaS 安全调查报告》以严谨的调研数据为基础，描绘出一幅生动而详实的 SaaS 安全画卷，为全球企业提供了应对 SaaS 安全挑战的实用洞察与决策依据。面对瞬息万变的网络安全环境，

企业应紧跟报告揭示的行业趋势，审视自身 SaaS 安全状况，适时调整策略与投资，以确保在数字化时代下，SaaS 成为驱动业务增长的稳健基石，而非潜在的风险源头

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

关键发现

1 SaaS 安全事件呈上升趋势

过去两年，55%的组织报告称经历过一次安全事件，另有 12%的组织表示不确定。调查结果强调，组织正在逐渐意识到一个严峻的现实，即勒索软件、恶意软件和数据泄露等针对本地部署类型的攻击也可能发生在 SaaS 云环境中。

2 当前的 SaaS 安全策略和方法还远远不够

调查发现，超过一半（58%）的组织认为，他们目前的 SaaS 安全解决方案只覆盖了 SaaS 应用程序的 50%或更少。而且他们越来越明显的感觉到，人工审计和 CASB 不足以保护组织免受 SaaS 安全事件的影响。

3 保护 SaaS 应用程序的利益相关者范围分散

随着 SaaS 应用程序的所有权分散到组织的各个不同部门，CISO 和安全管理者正在从控制者转变为管理者。协调、沟通和协作是确保组织 SaaS 全栈安全的关键。

4 组织如何为其整个 SaaS 安全生态系统确定策略和流程的优先级

SaaS 安全持续适应 SaaS 生态系统中不断扩大的广泛问题，包括 SaaS 错误配置、SaaS 与 SaaS 之间的访问、设备到 SaaS 的风险管理、身份和访问治理以及身份威胁检测与响应（ITDR）。组织正在制定强有力的策略、流程和能力，这对保护这些不同领域的安全性至关重要。

5 对 SaaS 和 SaaS 安全的投资正在急剧增加

66%的组织增加了对应用程序的投资，其中 71%的组织增加了对 SaaS 安全工具的投资。调查显示，SaaS 安全态势管理(SSPM)解决方案的采用率大幅增长，从 2022 年的 17%增长到 2023 年的 44%。这可以归因于 SSPM 提供了其他方法和策略无法覆盖的领域，通过在整个 SaaS 安全生态系统中提供更全面的保护以应对各种安全风险。

调查的开展与方法论

云安全联盟(CSA)是一家非营利组织，其使命是广泛推动云计算和 IT 技术领域的最佳实践，确保网络安全。同时，CSA 也就计算机相关的所有安全关注点对行业内各利益相关方展开教育。CSA 会员是由业内人士、企业和专业协会组成的广泛联盟。CSA 的主要目标之一是开展评估信息安全趋势的调查工作。这些调查提供组织当前在信息安全与技术领域的成熟度、观点、兴趣和行动等相关信息。

Adaptive Shield 委托 CSA 开展调查并编写相关报告，以便更好地了解行业关于 SaaS 应用程序使用、SaaS 安全策略和流程、SaaS 威胁以及 SaaS 安全战略/解决方案等方面的知识、态度和意见。Adaptive Shield 资助了此项目，并与 CSA 研究分析师联合设计了调查问卷。本次调查由 CSA 于 2023 年 3 月以在线方式开展，共收到 1130 份来自不同规模和地区组织的 IT 和安全专家的答卷。CSA 的研究团队对本报告进行了数据分析和解读。

研究目标

本次调查的主要目的是为了更深入地了解组织中 SaaS 安全的几个关键方面。

- 当前 SaaS 应用程序在组织中的使用情况
- 组织有关 SaaS 应用程序的安全策略和流程
- 对 SaaS 威胁的认识和经验
- 当前和未来使用的安全解决方案

数据&探讨

在当今的数字环境中，SaaS 安全性对各种规模的组织都至关重要。随着企业越来越多地将其操作和数据转移至云端，或者更具体地说是 SaaS 应用程序，这些应用程序的安全性变得尤为重要。虽然 SaaS 应用程序在设计上是安全的，但它们的配置和管理方式会带来风险。如果缺乏适当的安全措施，组织将会面临数据泄露、网络攻击和其他可能导致重大财务和声誉损失的安全事件。因此，了解 SaaS 安全性对于组织保护自身免受这些风险至关重要。

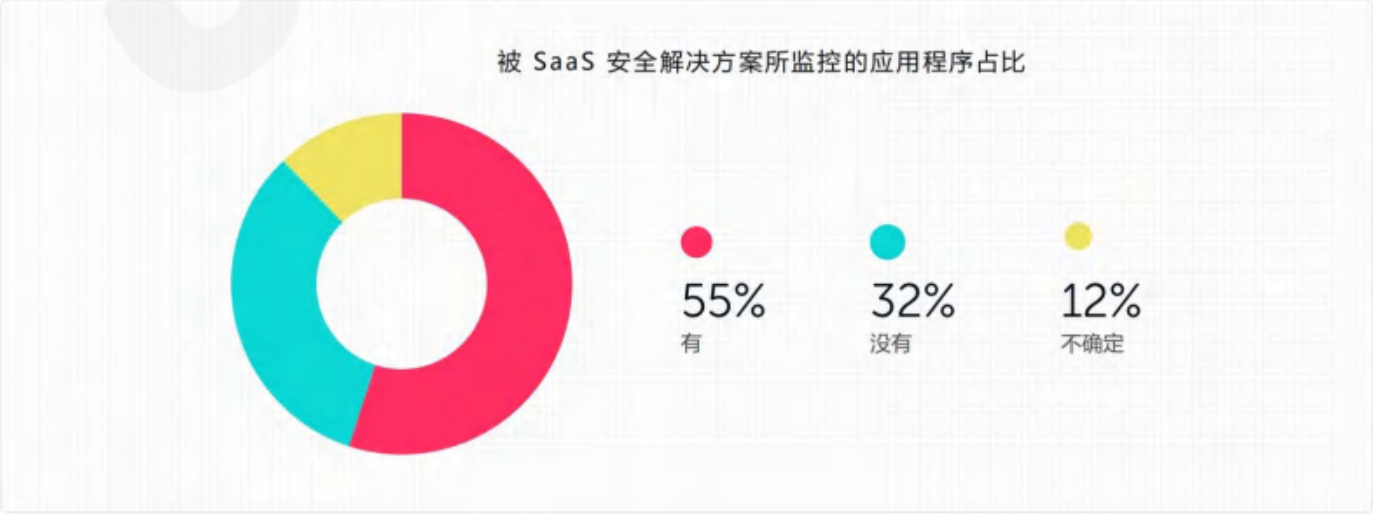
正是在这样的背景下，云安全联盟（CSA）发布了《年度 SaaS 安全调查报告》，深入探讨了 SaaS 安全的复杂性，并提供了去年报告的后续内容。以下是今年的调查结果和见解。

关键发现 #1

SaaS 安全事件呈上升趋势

调查显示，SaaS 生态系统内的安全事件显著增加，55%的组织报告说他们在过去两年内经历过安全事件，比去年增加了 12%。大约三分之一(32%)的受访者表示，他们在同一时期内没有遭遇过 SaaS 安全事件，而 12%的受访者表示不确定。

调查结果强调，许多公司开始认识到一个严峻的现实，即常见的针对本地部署类型的攻击，如勒索软件、恶意软件和数据泄露，也可能发生在他们的 SaaS 云环境中。



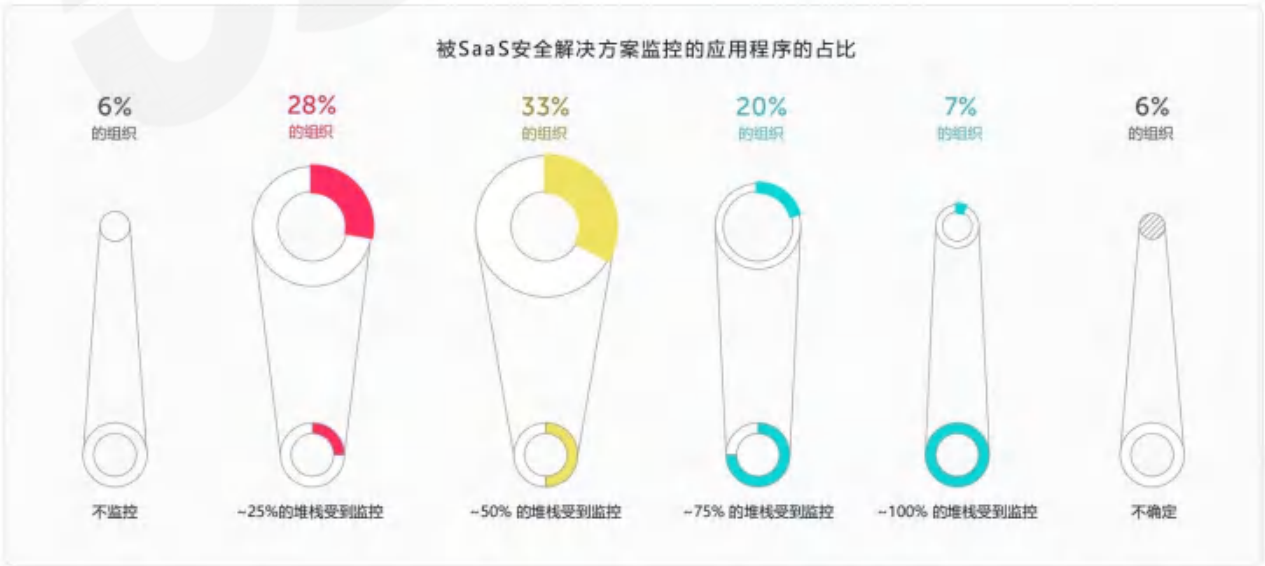
报告中最常见的 SaaS 安全事件包括数据外泄 (58%)、恶意应用 (47%)、数据泄露(41%)和 SaaS 勒索软件(40%)，这凸显了对强大安全措施的需求日益增长，以及对 SaaS 领域不断扩大的潜在风险的认识不断提高。

关键发现 #2

当前的 SaaS 安全策略和方法还远远不够

对 SaaS 应用程序的监控不足

调查结果表明，大量组织在实施有效的 SaaS 安全措施方面存在不足，这是 SaaS 安全事件显著增加的一个关键原因。许多公司使用的安全解决方案并未涵盖整个 SaaS 堆栈，这使得他们的应用程序和数据暴露在网络威胁之下。具体来说，调查发现，超过一半 (58%) 的组织估计他们当前的 SaaS 安全解决方案仅覆盖了 SaaS 应用程序的 50%或更少。



这些发现凸显了公司迫切需要重新评估它们的安全解决方案，并确保这些解决方案能为其整个 SaaS 生态系统提供全面的覆盖。这样，组织才可以显著降低他们各类安全事件的风险，包括数据泄露，勒索软件攻击，以及其他类型的网络攻击。最后将有助于维护他们的声誉和维系客户的信任。

CASBs 和人工审计达不到 SaaS 安全的要求

许多组织依赖云访问安全代理（CASB）和人工审计来保护其 SaaS 应用程序。然而，这些方法在一些关键领域是不够的。此外，人工审计会将公司数据暴露给审计师，使组织在这些审计期间面临发生安全事件的风险。

这些发现表明，组织需要重新评估他们的安全策略并在更具综合性的解决方案和策略方面进行投入，以便为其 SaaS 生态系统提供全面的覆盖来降低安全事件的风险。这也是导致 SaaS 安全态势管理（SSPM）工具使用增加的原因。

关键发现 #3

保护 SaaS 应用程序的利益相关者范围分散

除了对工具、安全和员工的现金投资外，组织还让越来越多的利益相关者参与到保护业务关键应用程序的过程中。一个典型的组织，都有广泛的 SaaS 应用，从文件共享和协作应用程序到 CRM，项目和工作管理应用，市场营销自动化应用，等等。SaaS 应用程序承载了各种利益角色，但这种利益相关者的分散使威胁形势变得复杂。

现在，CISO（首席信息安全官）和安全经理正在从 SaaS 应用程序的控制者转向管理者。调查显示，从事安全治理的人员中有不少人担任行政职位或部门主管，这表明企业正在认真对待 SaaS 安全。关键决策者的参与表明人们越来越认识到 SaaS 安全在保护有价值的资产和确保运营连续性方面发挥的关键作用。

然而，参与的人越多，确定谁最终负责 SaaS 安全可能变得越难。SaaS 应用程序通常需要安全团队和应用程序所有者之间的密切协作，因为安全团队通常并不能够直接访问 SaaS 应用程序。这就需要能够弥合差距并积极吸引应用程序所有者的流程和工具，他们对于有效的 SaaS 安全管理至关重要。

在安全团队和应用程序所有者之间的沟通和协调中，通过搭建一套协作环境和实施解决方案或策

略，组织可以形成一个更为健壮和更加精简的方法来保护他们的关键业务应用程序。相应的，这也有助于减少潜在的威胁，并确保对 SaaS 安全威胁提供更高水平的防护。

关键发现 #4

组织如何为其整个 SaaS 安全生态系统确定策略和流程的优先级

在过去的一年里，在过去的一年里，SaaS 安全的焦点发生了显著的变化，这主要是由于对业务关键型 SaaS 应用程序的投资增加、安全事件的增加以及针对 SaaS 应用程序的威胁角色增加等因素造成的。以前，以 SSPMs 为代表的组织和安全工具，主要关注错误配置管理。然而，SaaS 安全已经有了更广泛的关注范围，包括 SaaS 与 SaaS 之间的访问、设备到 SaaS 的风险管理、身份和访问管理，以及身份威胁检测和响应（ITDR）。

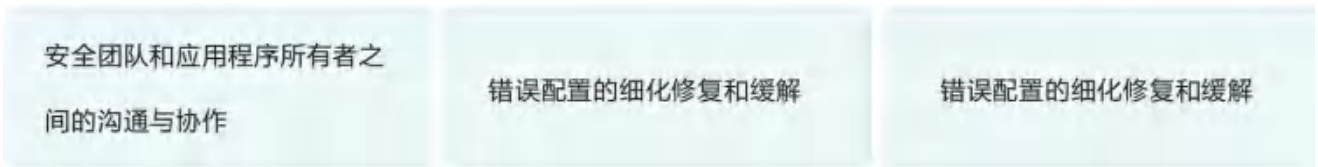
SaaS 策略和程序

随着 SaaS 在业务领域中的重要性日益上升，拥有健壮的策略、流程和适当的能力对于保护组织的 SaaS 堆栈及其包含的数据不受威胁影响至关重要。

各组织目前正在采取措施解决关键领域的问题。以下数据显示了组织在 SaaS 安全生态系统的不同领域中保护其 SaaS 堆栈时开始优先考虑的内容。

错误配置管理

解决错误配置问题对于保护组织的 SaaS 堆栈免受可能被威胁行动者利用的、配置错误的安全设置至关重要。受访者认为错误配置的详细修复和缓解措施包括：



有了强大的系统和流程，这些高影响的领域可以帮助减少 SaaS 攻击面。

第三方应用程序访问

随着组织越来越依赖于第三方 SaaS 应用程序(连接到核心堆栈)，制定评估和管理潜在风险方面的政策变得尤为重要。第三方应用程序访问的主要优先事项包括：

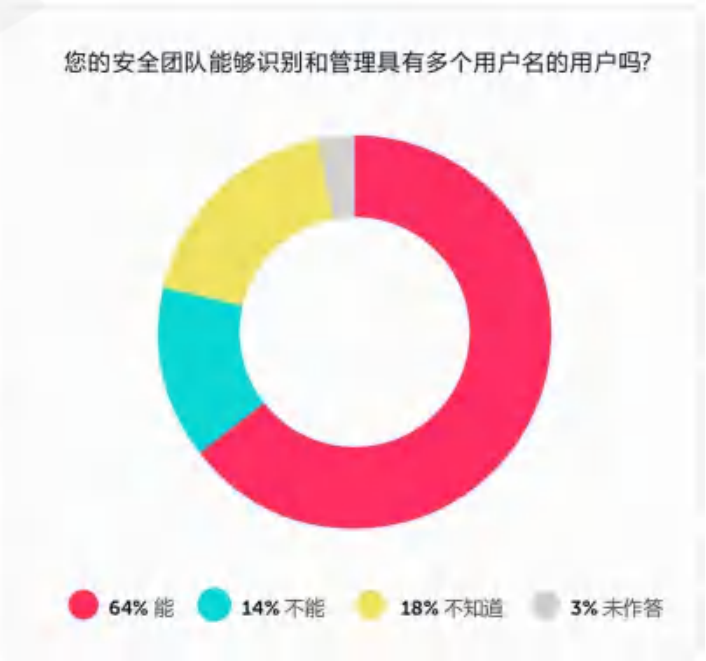
对已连入的第三方SaaS应用程序的风险的识别、检测和量化	检测已经集成到SaaS堆栈中的恶意应用程序	要求应用程序所有者在连接一个应用程序之前向安全部门提交请求

这些优先事项表明需要建立强大的系统和流程，以防止第三方应用程序的访问威胁。

SaaS 身份和访问治理

恰当的身份和访问治理对于保护 SaaS 生态系统中的敏感数据至关重要。当前涉及组织中的身份和访问治理的优先事项包括：

- 确保每个用户都有所需的正确的访问级别
- 检测在活动目录中已被禁用但仍然可以访问SaaS应用程序的用户
- 检测休眠账户，以便在需要时可以快速取消其对SaaS的访问权限
- 管理访问通知
- 身份验证实践（例如，密钥管理、证书管理）



监控 SaaS 用户设备

确保访问 SaaS 堆栈的设备的安全性，这对于防止未经授权的访问和数据泄露至关重要。为了确保 SaaS 风险不源于设备，组织的优先事项包括：

检查每个SaaS用户，尤其是特权用户的设备安全情况（漏洞和更新的代理）。	识别访问SaaS堆栈中的未受管理的设备。

许多人并不认为设备是 SaaS 应用程序安全性中的一个弱点。但事实恰恰相反，设备是一个入口。如果特权用户的设备不安全，一旦威胁被成功利用，那么造成的损害将是巨大的。

威胁检测和响应

积极主动的威胁检测和响应对于保护组织免受有针对性攻击至关重要。在当今的环境中，威胁检测和响应的优先事项包括：

对用户和实体的行为异常进行识别和响应	检测多因素身份验证（MFA）洪水攻击
通过威胁情报检测攻击	检测暴力破解攻击

关键发现#5

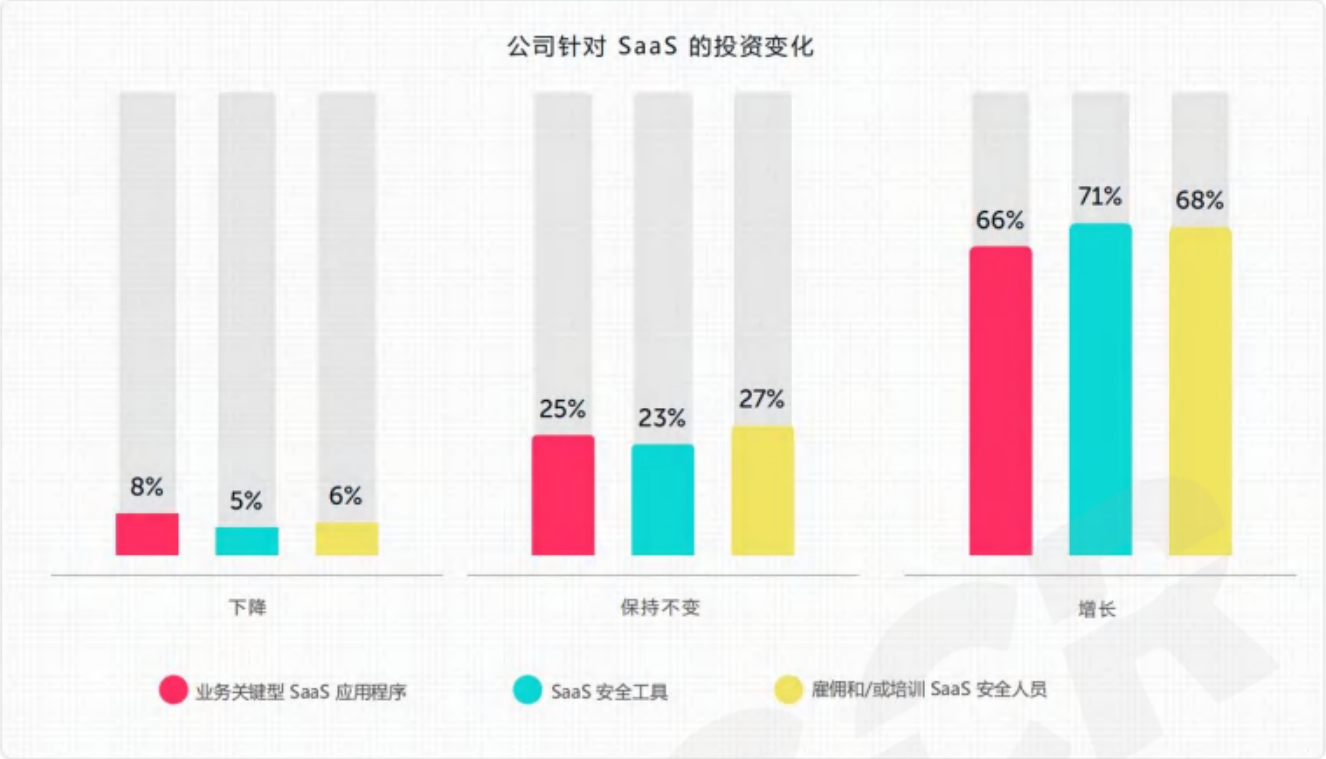
对 SaaS 和 SaaS 安全的投资正在急剧增加

对 SaaS 增加的投资

组织越来越严重的依赖 SaaS 资源，这不仅涵盖关键业务应用程序和人员，还包括专注于 SaaS 安全的合适的安全工具。

根据调查，71%的组织增加了对 SaaS 安全工具的投资，表明其致力保护数字资产的决心。此外，68%的组织加大了在 SaaS 安全方面雇佣和培训员工的投资，表明他们意识到人力资本在保护其 SaaS 生态系统中的重要性。此外，66%的组织增加了他们对业务关键型 SaaS 应用程序的投资，反映了在核心业务功能中对这些工具的日益依赖。

这种对 SaaS 投资的整体性策略，包括安全工具、人员和应用程序，凸显了强大的安全解决方案（如 SSPMs）的重要性。



SaaS 安全态势管理（SSPM）的使用增加

随着 SaaS 安全事件的增加和当前的 SaaS 安全方法（如 CASB 和人工审计）的不足，组织正在寻找更先进的 SaaS 安全工具，如 SSPM。调查显示，采用 SSPM 工具的组织数量显著增长，从 2022 年的 17%增加到 2023 年的 44%。

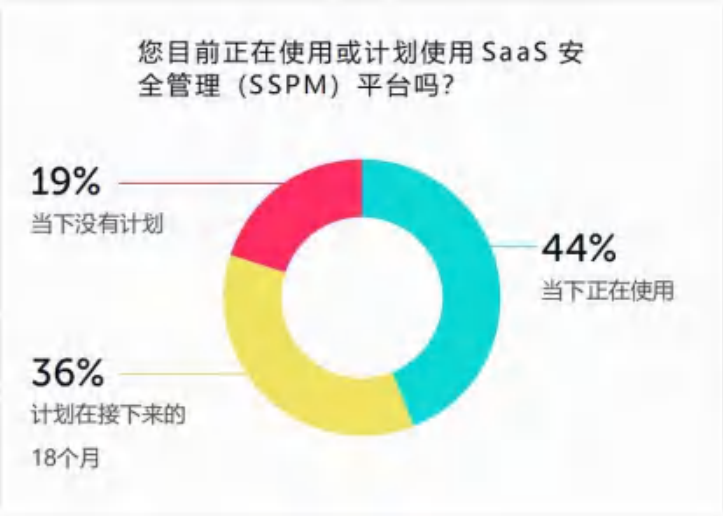
这可以归因于 SSPM 弥补了其他方法和策略的不足，为整个 SaaS 安全生态系统提供了更全面的保护，从而应对各种安全风险。

现将本文详细描述的领域总结如下：

- **SaaS 配置错误：**确保 SaaS 应用程序的正确配置以避免违规。
- **身份和访问治理：**管理和控制用户对 SaaS 应用程序和资源的访问。
- **第三方应用程序访问：**识别并管理与第三方应用程序访问 SaaS 环境的相关风险。
- **数据丢失管理：**预防和减轻 SaaS 应用中敏感数据的丢失或泄漏。
- **连接的恶意应用：**检测和移除可能危及 SaaS 环境安全的恶意应用程序。

- **威胁检测与响应：**实时主动识别和应对安全威胁。
- **SaaS 用户设备：**监控和管理用户设备连接 SaaS 应用时的相关安全风险。

随着 SaaS 安全事件的不断增加，组织越来越意识到 CASB 和人工审计等其他安全方法的局限性。已经采用或计划采用 SSPM 解决方案的组织占比越来越高，这表明人们越来越意识到需要更健壮、更全面的安全措施，以抵御不断发展的 SaaS 安全威胁。



SSPM 的优势

随着 SaaS 安全的重要性日益增加，采用更全面和强大的手段非常必要。SSPM 等 SaaS 安全工具可以帮助组织应对当今 SaaS 安全领域所需的政策、流程和能力。通过专注于这些关键方面，组织可以更好地保护其宝贵的资产，并在日益复杂的威胁环境中确保业务关键型应用程序的安全。

组织越来越意识到采用 SSPM 等 SaaS 安全工具应对 SaaS 安全挑战的价值。这就解释了为什么有 44%的组织在过去一年中已经采用了 SSPM 解决方案，以及为什么有 36%的组织计划在未来 18 个月内采用 SSPM。通过利用这些工具，企业可以有效地减轻 SaaS 威胁，并显著提升整体安全态势。

此外，使用 SSPM 可以使得组织在管理和维护方面节约时间，因为这些解决方案可以简化并自动化各种安全流程，而这些流程在没有自动化之前需要手动完成。这种自动化不仅可以通过减少手动操作来实现成本节省，还可以使组织将资源重新分配到其他关键领域。此外，SaaS 安全工具提供了应对新条件和新兴威胁所需的适应性，确保企业在不断变化的环境中保持敏捷，并做好保护其数字资产和关键应用程序的准备。

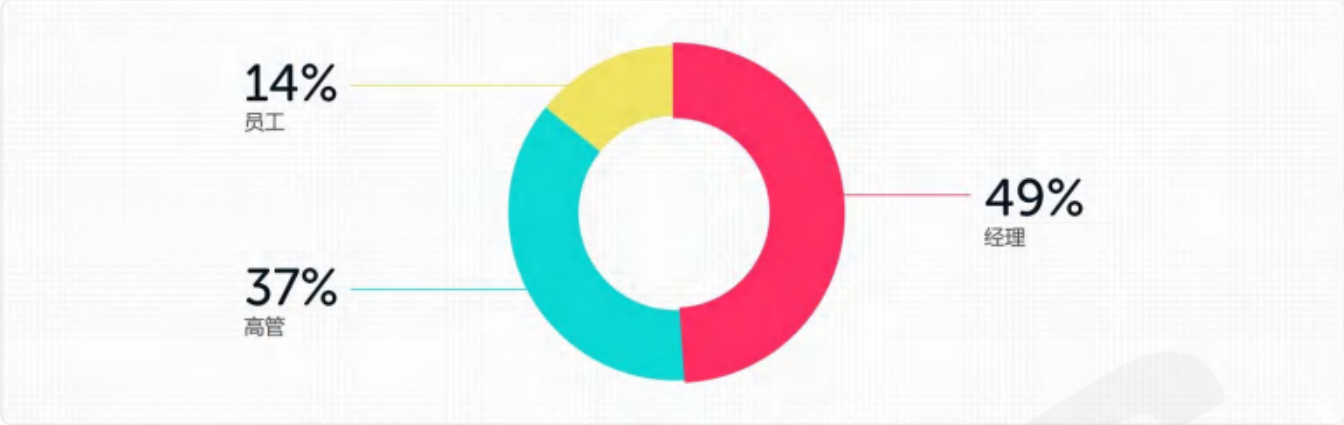
人口统计

该调查由 CSA 于 2023 年 3 月在线进行，收到了来自不同规模和地点的相关组织的 IT 及安全专业人员共计 1130 份回复。

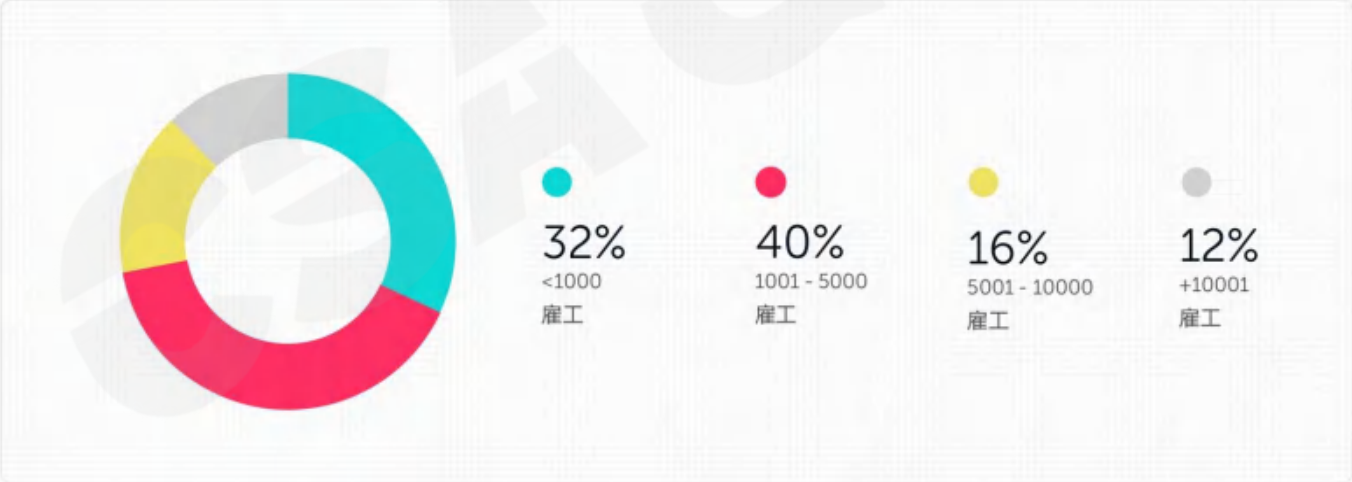
你在哪个行业工作？

以下哪一项最符合您的角色？

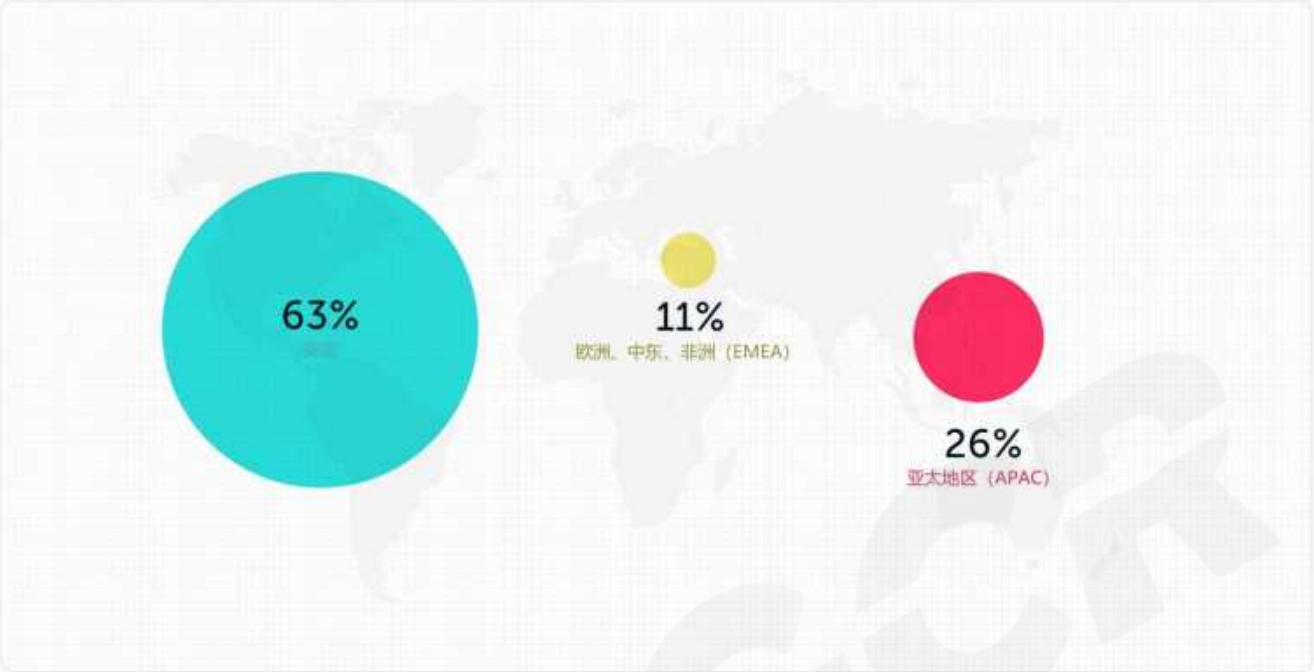
您的工作水平如何？



您的组织的规模是多大？

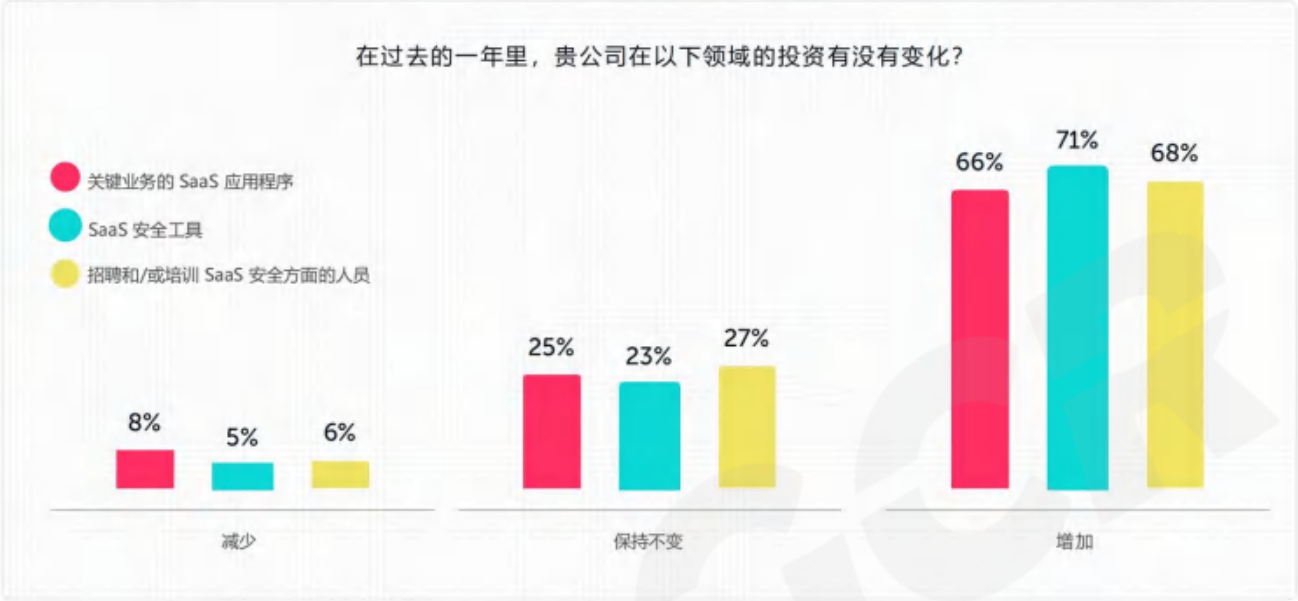


你位于世界的哪个地区？

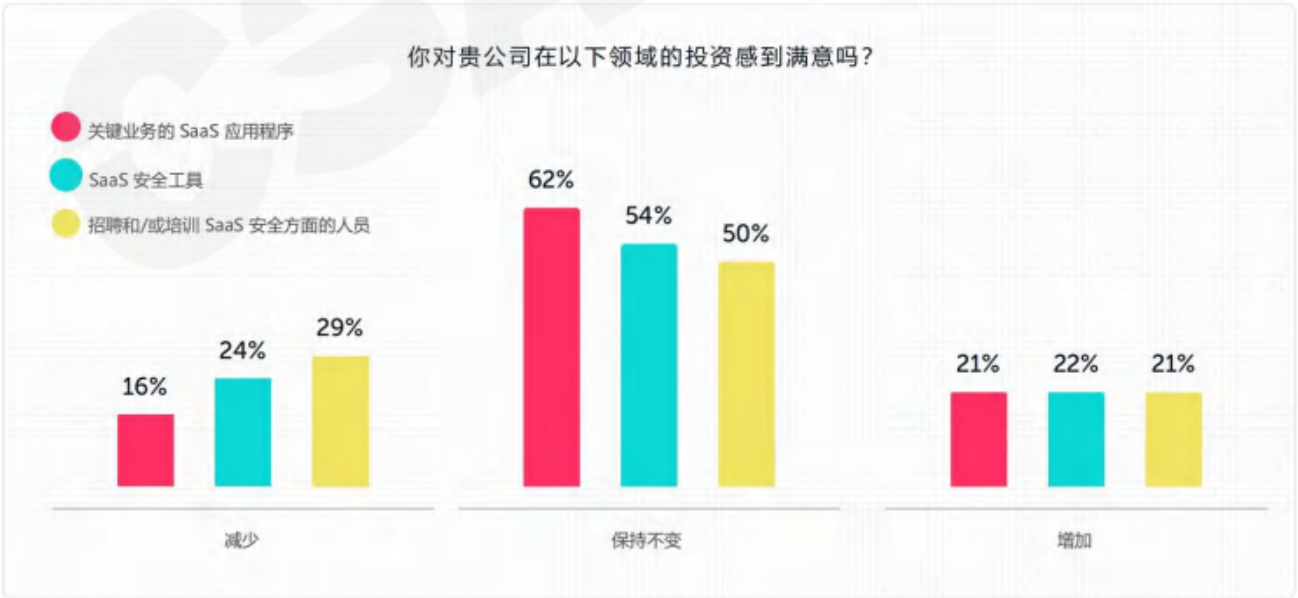


附录 A：调查结果

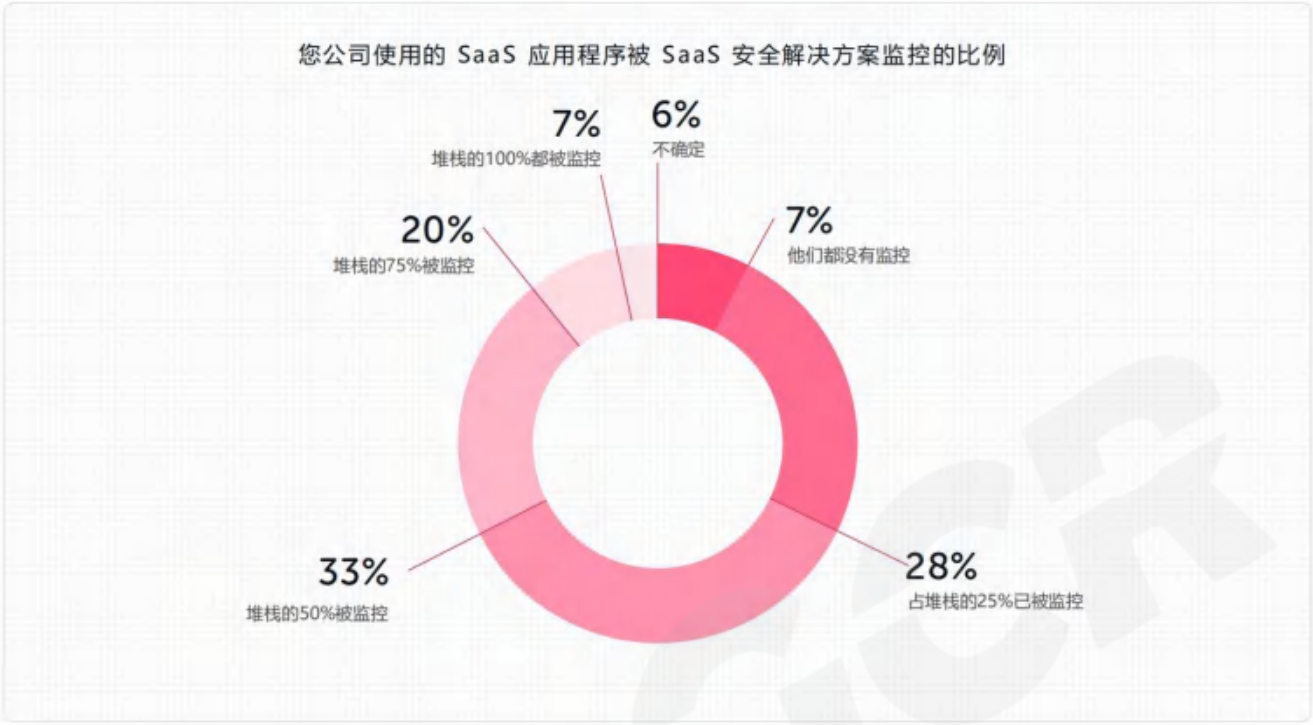
公司 SaaS 投资的变化



公司对 SaaS 投资的满意度



由 SaaS 安全解决方案监控的 SaaS 应用程序占比



保护业务关键型应用程序所涉及的工作角色

最重要的安全问题

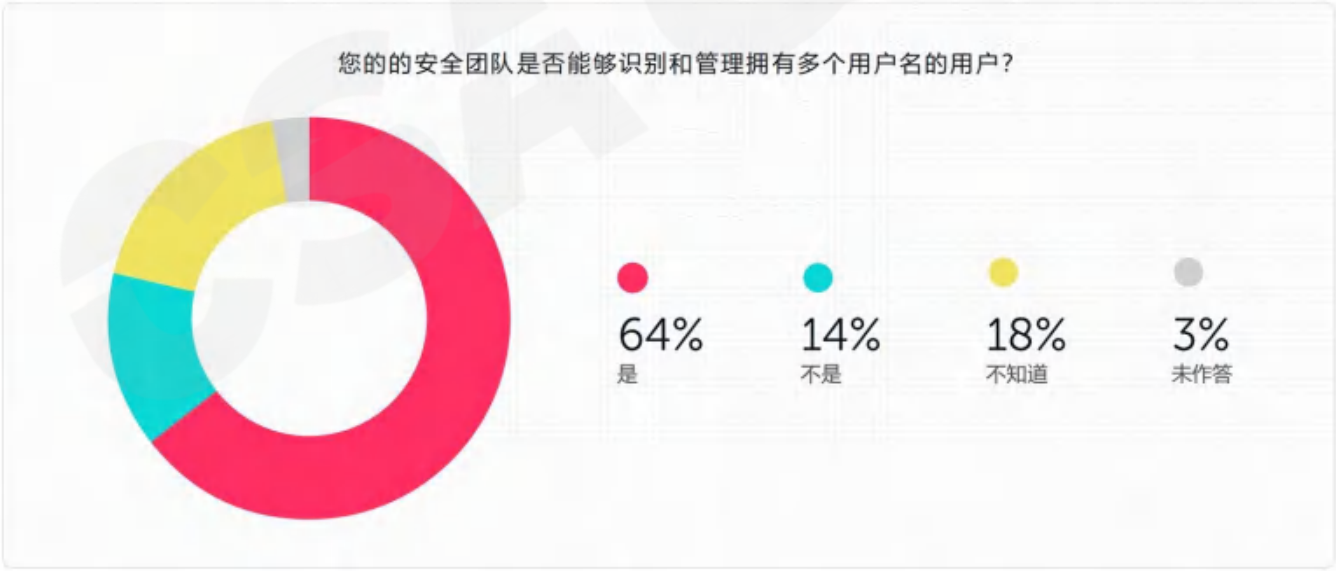
SaaS 安全策略和流程

在这部分，受访者被要求选择所有适用的答案

错误配置管理

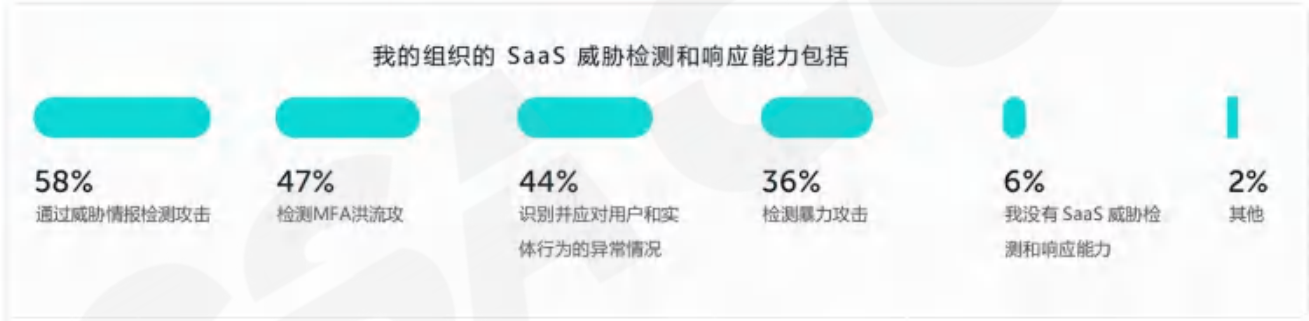
第三方应用程序访问核心 SaaS 堆栈

身份和访问治理



对访问 SaaS 应用程序的设备的监控

针对 SaaS 威胁的检测和响应能力

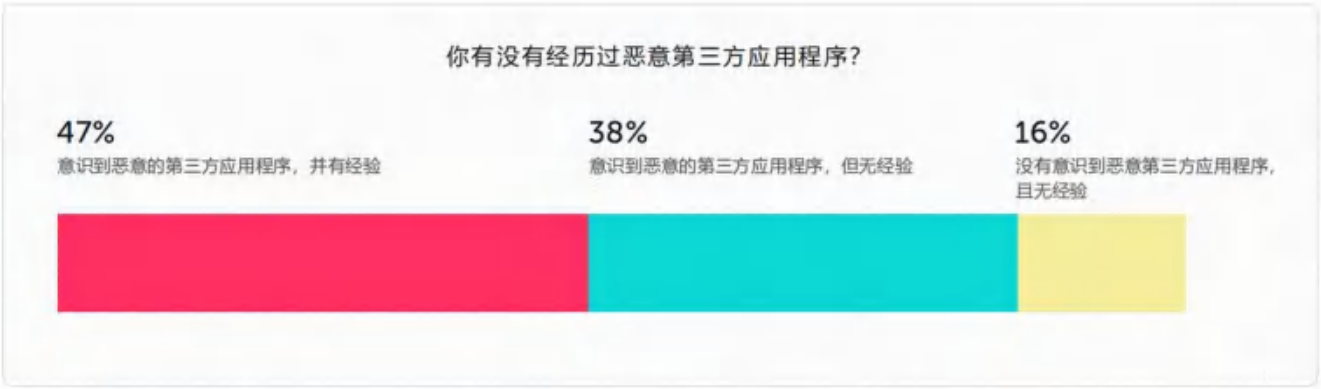


关于 SaaS 安全的数据丢失预防

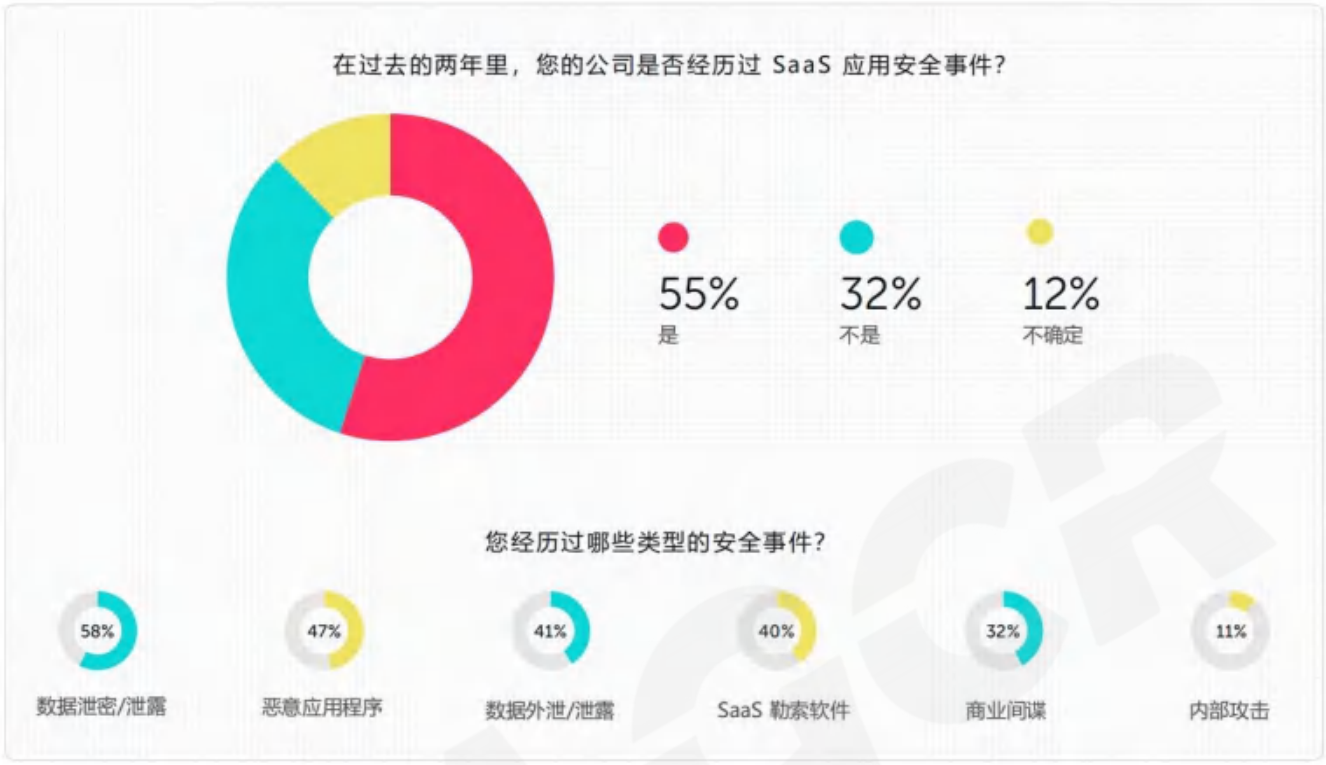
SaaS 威胁

CASB 对 SaaS 的覆盖

人工审计对 SaaS 应用程序的覆盖范围



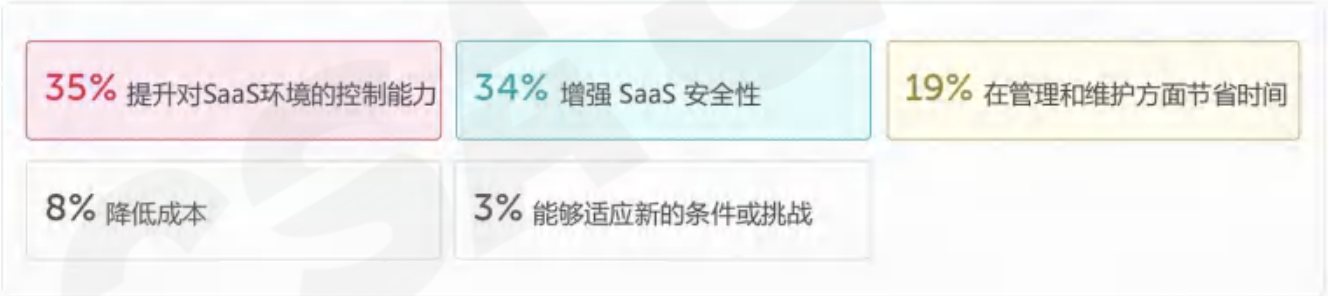
SaaS 应用安全事件



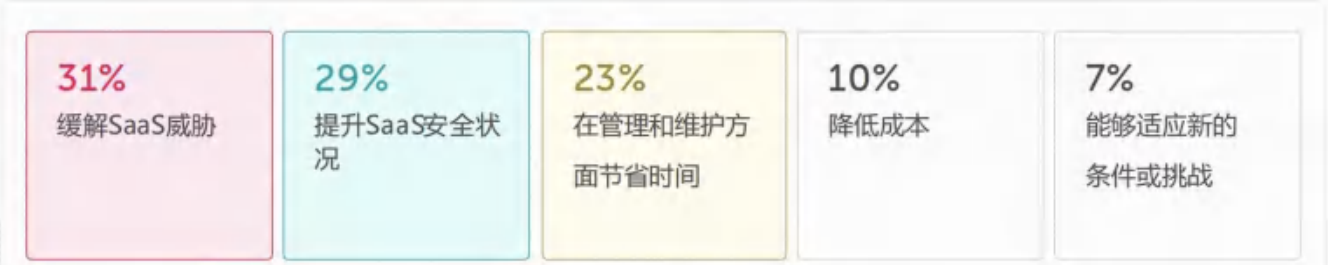
SSPM 的使用和优势

正在使用或计划使用 SSPM

SSPM 使用的主要优势

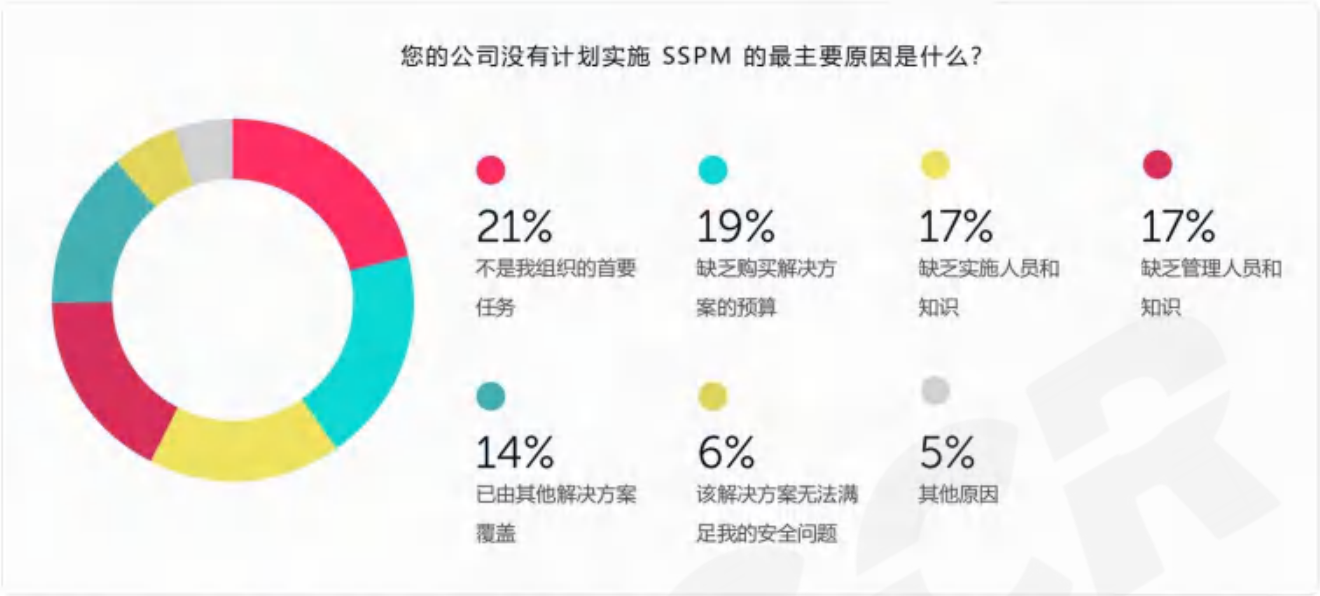


预期从 SSPM 解决方案中获得的主要优势



计划在接下来的 18 个月内实施 SSPM 解决方案的调查结果

不实施 SSPM 的原因



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