2022 SaaS 安全调查报告

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

序言

从Salesforce 1999年发布CRM SaaS 服务成为SaaS的开拓者，到2022年全球企业服务SaaS市场规模将超1700亿美元（据Statista预测），SaaS成了真正的“软件终结者”。国内SaaS虽然起步较晚但也已经在2019年进入了旺盛期，CRM、ERP、HCM、OA、财务、客服、电子签等垂直领域的SaaS蓬勃发展。而且几乎所有传统的管理软件企业都开始了新一轮的转型尝试。新冠疫情爆发以来，很多企业不得不选择远程办公和使用线上SaaS应用，疫情成了SaaS发展的又一个助推剂。

SaaS快速发展的同时也面临不少安全问题，这些问题已经成为很多组织关注的焦点。CSA继发布CAST云应用安全可信标准与认证之后，就SaaS安全相关的问题开展调查并发布了《2022 SaaS安全调查报告》（以下简称《报告》）。调查从收集到的340份来自不同规模组织和地区的IT/安全专家的答卷中深入挖掘，筛选出了5大关键的安全问题，并对其产生的原因进行了研究与分析，通过一系列数据说明了这几大问题的普遍性与严重性。值得关注的是在本次调查过程中，云平台上流窜的病毒、木马、网络攻击已不再是最主要的安全风险，错误配置、权限模糊、安全减配等管理问题已经成为企业SaaS安全管理过程中必须慎重对待的关键问题。

作为企业的 IT管理人员，尤其是信息安全管理人员，应该清楚地知道：没有安全事故不等于足够的安全。那如何保证企业在日益复杂的网络环境下的数字安全，保证云上业务的安全？这些问题在《报告》中也给出了相对应的解决思路。除此之外，《报告》中的一些对比数据或许可以为企业解决SaaS安全问题提供借鉴，给企业的使用SaaS带来一些启示。对于很多企业来说，安全地使用SaaS是一个很有挑战的过程，需要加强企业内部的控制策略，并通过统一的安全保障措施和策略对SaaS应用进行识别和管控。同时推荐使用SSPM管理，为安全团队提供SaaS应用程序安全设置可见性的能力，也可以利用自动化工具监控和修复SaaS安全错误配置。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致谢

《2022 SaaS 安全调查报告》（2022 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：侯 俊 朱梦婷 薛 琨 王永霞

审校组：郭鹏程、姚凯

研究协调员：江瞿天

感谢以下单位对本文档的支持与贡献：

北京北森云计算股份有限公司 深圳市魔方安全科技有限公司

网宿科技股份有限公司 腾讯云计算（北京）有限责任公司

英文版本编写专家

主要作者：Hillary Baron Josh Buker Sean Heide Alex Kaluza Shamun Mahmud John Yeoh

设计师：Claire Lehnert Stephen Lumpe

特别鸣谢：Eliana Vuijsje Caroline Rosenberg at Adaptive Shield

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秘书处给与雅正!

联系邮箱research@c-csa.cn；国际云安全联盟CSA公众号。

目录

调研的开展与方法论

云安全联盟（CSA）是一家非营利性组织，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也就计算机技术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，这些调查提供的与企业组织在信息安全与技术领域的成熟度、观点、兴趣和行动相关的信息。

Adaptive Shield（以色列SaaS应用安全服务商）委托CSA开展调查并编写相关的报告，以便更好地了解关于SaaS安全和相关错误配置的行业知识、态度和意见。Adaptive Shield资助了本项目并与CSA的研究分析师联合设计了调查问卷。本次调查从2022年1月至2月，由CSA以在线方式开展，共收到340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

本调查的目标是了解当前SaaS安全和错误配置状况。关注的关键领域包括：

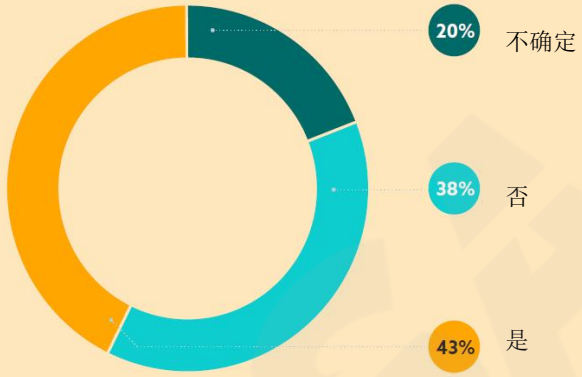
- 使用SaaS应用的企业组织
- 评估SaaS应用程序安全的方法、策略和工具
- 检测和修复SaaS应用程序安全里错误配置的时间表
- 了解SaaS安全相关的最新产品

概要

许多最近发生的违规与数据泄露事件由错误配置导致，使其成为众多企业组织关注的焦点。多数关于错误配置的研究只关注IaaS层，而忽略了SaaS全栈。然而，SaaS安全和错误配置对于企业的整体安全同等重要。基于上述原因，CSA设计并发布了一项调查，以便更好地了解SaaS应用的使用，SaaS安全性评估的工具与时间表，检测和修复错误配置的时间表，以及对SaaS应用相关安全工具的认识了解。

关键发现 1
SaaS错误配置导致安全事件

至少自2019年[1]起，错误配置就已经成为组织关注的重点。不幸的是，至少43%的组织经历过一个或多个因SaaS错误配置引发的安全事件。此外，一些组织曾经历过安全事件，但不确定是否归结于SaaS的错误配置，否则这一比例将高达63%。与17%的组织因IaaS错误配置而遭遇安全事件相比，这一数据就显得尤为突出。[2]



因此，组织需要采取自动化和持续扫描措施，不仅针对IaaS的错误配置，还应包括SaaS的错误配置，以防止安全事件发生。自动化措施能使组织实时修复该问题，从而避免留下隐患。

关键发现 2
导致SaaS错误配置的主要原因是缺少可见性以及具有访问权限的部门太多

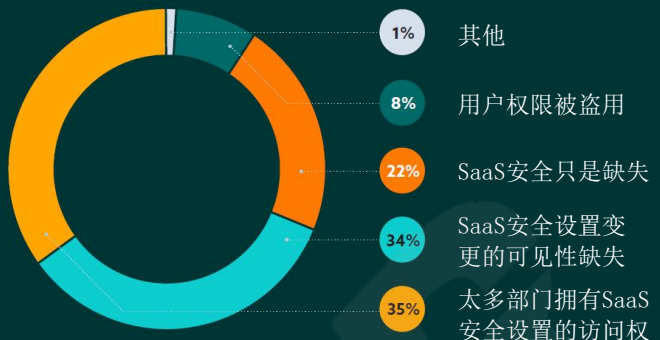
安全事件的主要原因来自两个方面：太多部门拥有SaaS安全设置的访问权限（占比35%），以及对SaaS安全设置的变更缺少可见性（占比34%）。这一发现并不令人惊讶，原因有二：1.选择SaaS应用时，安全设置可见性的缺失被评为首要问题。2.通常，组织内有多个部门具备访问这些安全设置的权限（详见“为SaaS应用安全设置负责”部分）。

[1] 云计算面临的11类顶级威胁. (CSA) 2019.

[2] 云安全风险、合规和错误配置的状况. (CSA) 2021.

有40%的组织认为，访问SaaS应用程序的部门是业务部门（如法务、市场、营销），目的是执行工作相关的任务。通常情况下，这些部门缺少适当的培训和对安全设置变更的关注。

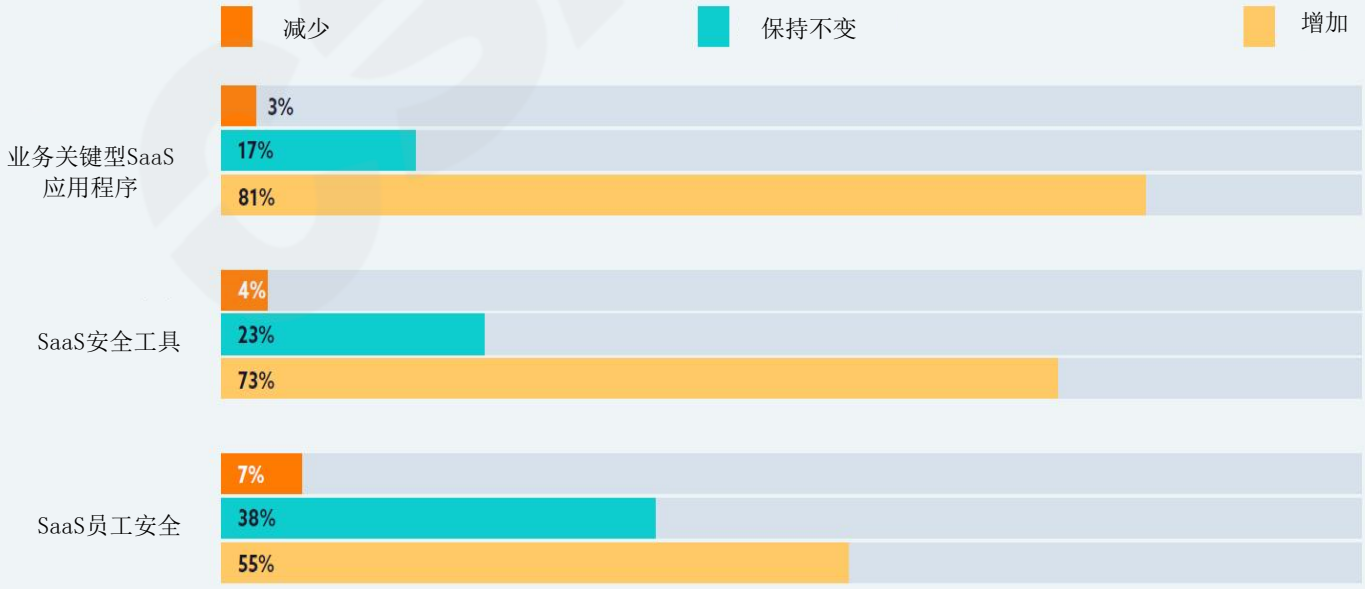
然而，他们完成工作需要这种级别的SaaS应用访问权限。这意味着组织需要为多个部门启用访问权限，并为安全团队提供安全设置变更的洞察能力。



关键发现 3
对业务关键型SaaS应用的投入超过SaaS安全工具和人员的投入

一年以来，有81%的组织对业务关键型SaaS应用增加了投入，但是相比之下，较少组织表示他们为了SaaS安全，在安全工具（73%）和人员（55%）方面增加了投入。这一变化意味着，现有安全团队负担了更多SaaS安全监控的责任。在另一个关键发现中可以看到，安全团队采用自动化技术监控SaaS安全，能帮助减轻压力，但是只有26%的组织使用该项技术。

安全团队正在花费更多时间，以手工方式评估安全，检测和修复错误配置。组织在业务关键型SaaS应用进行投入时，必须考虑这种情况，因为当前投入模式从长期来看不可持续。

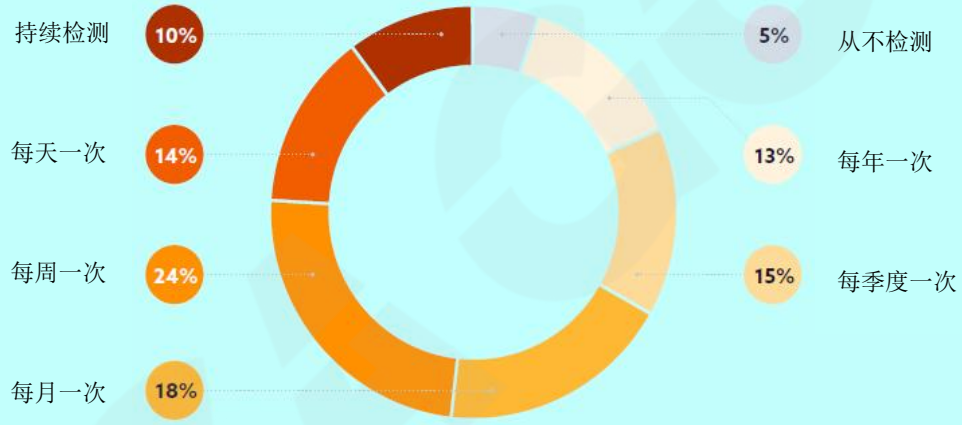


关键发现4

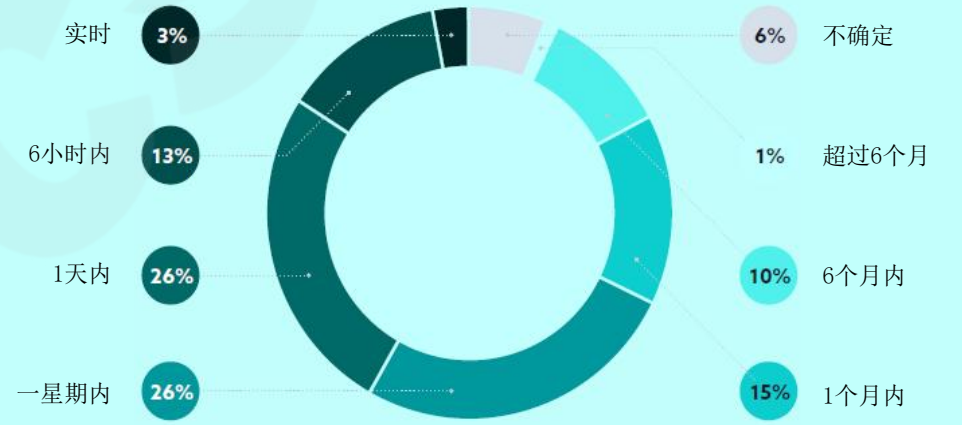
人工检测和修复SaaS错误配置的方式使企业暴露于风险之中

人工检测和修复不安全配置的方式不仅给安全团队带来负担，其滞后性也给企业增加了风险。近半数（46%）企业对SaaS安全配置的检查频率为每月一次或更低，5%的企业甚至完全不检查。这个数据意味着不安全的配置在一个月乃至更长的时间内放任不管。即使企业发现存在不安全配置的情况，还需要额外的时间修复，约1/4的企业需要一周或更长的时间手动修复错误配置，在此期间企业将处于风险之中。为了避免由于SaaS错误配置导致的安全事件的发生，企业必须探索自动化的方式或其他类似的工具缩短检测和修复错误配置的时长。

SaaS安全配置检测频率



修复SaaS错误配置所需的时间



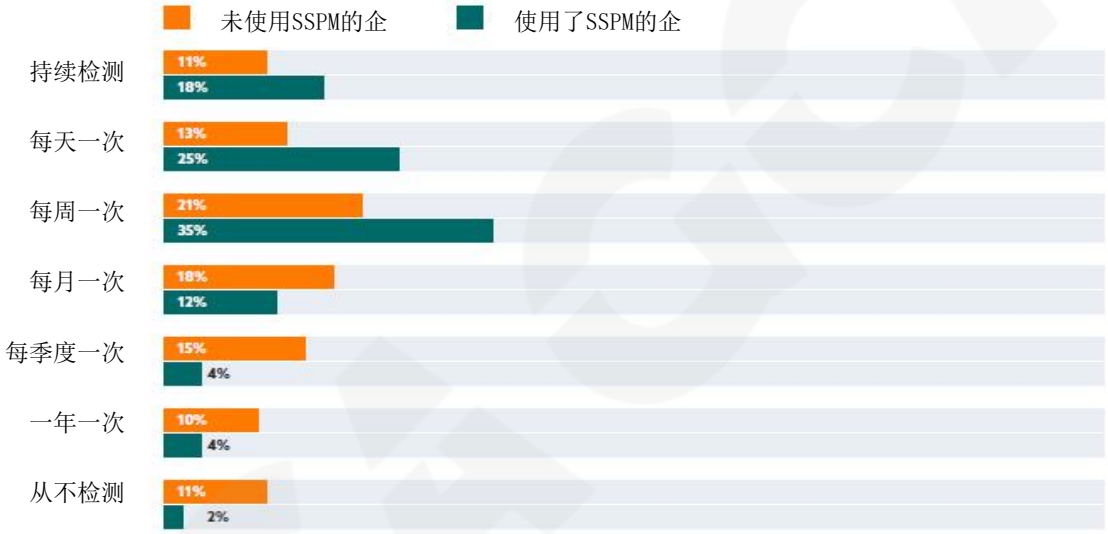
*该数据仅统计人工检测及修复的情况

关键发现5

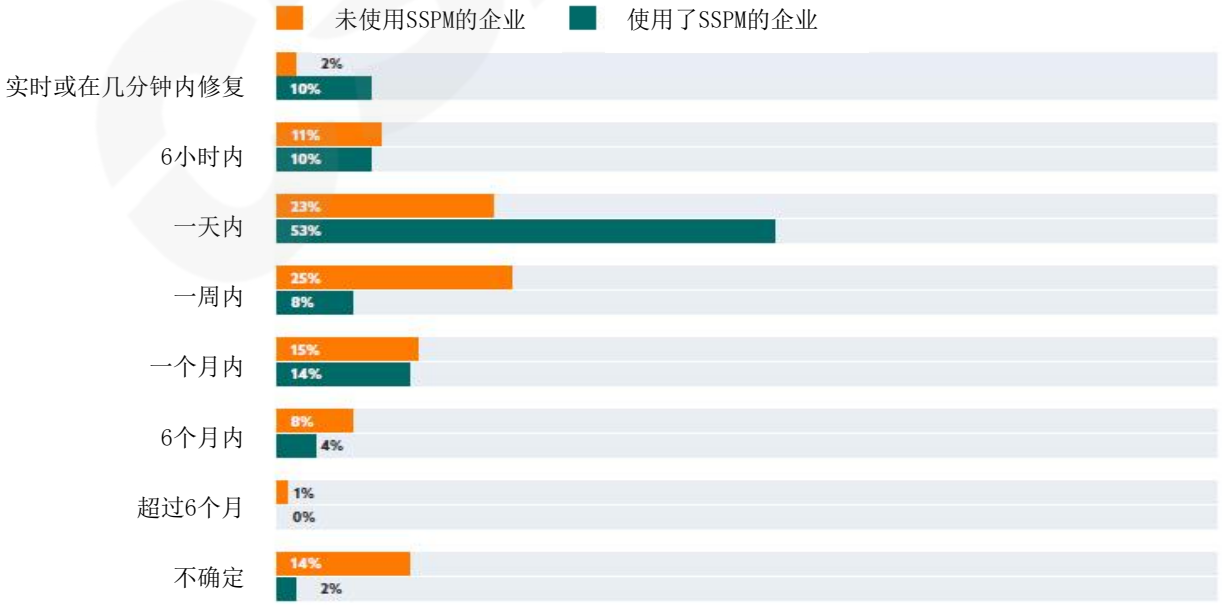
SSPM的应用有助于缩短SaaS错误配置检测及修复时长

使用SSPM解决方案的企业能够更快地检测及修复SaaS错误配置。大多数（78%）企业每周或更频繁地检测，而那些没有使用SSPM的企业中只有45%能够达到同样的检测频率。在错误配置的修复上，使用SSPM的企业中的73%能够在一天内修复问题，81%能够在一周内修复。反观那些没有使用SSMP的企业，只有35%能够在一天内修复，61%在一周内修复。结合这些数据不难看出，使用了SSPM的企业能够缩短在安全风险中的暴露时间。

SaaS安全配置检测频率



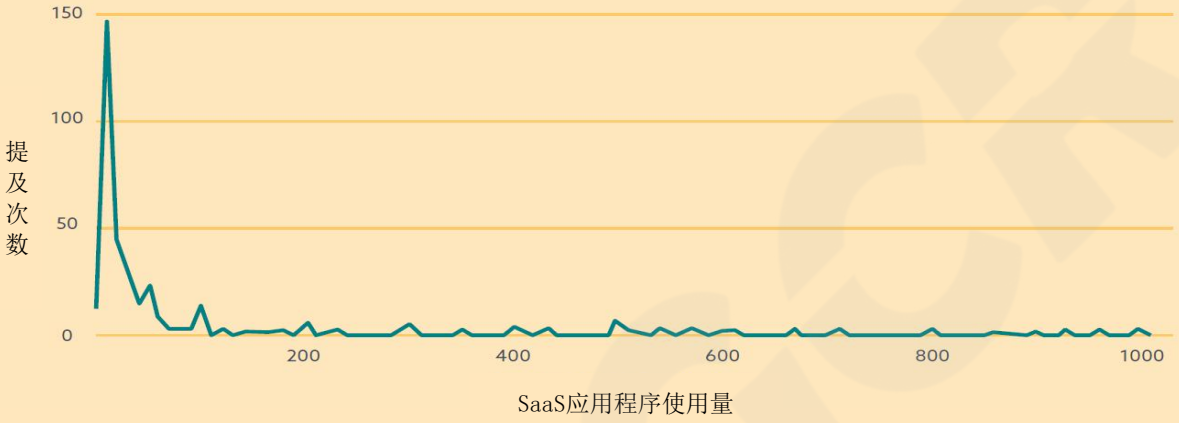
修复SaaS错误配置所需的时间



企业的SaaS应用程序使用情况

企业的SaaS应用程序使用量（预估）

单个企业平均使用102个SaaS应用，最多的超过5000个。

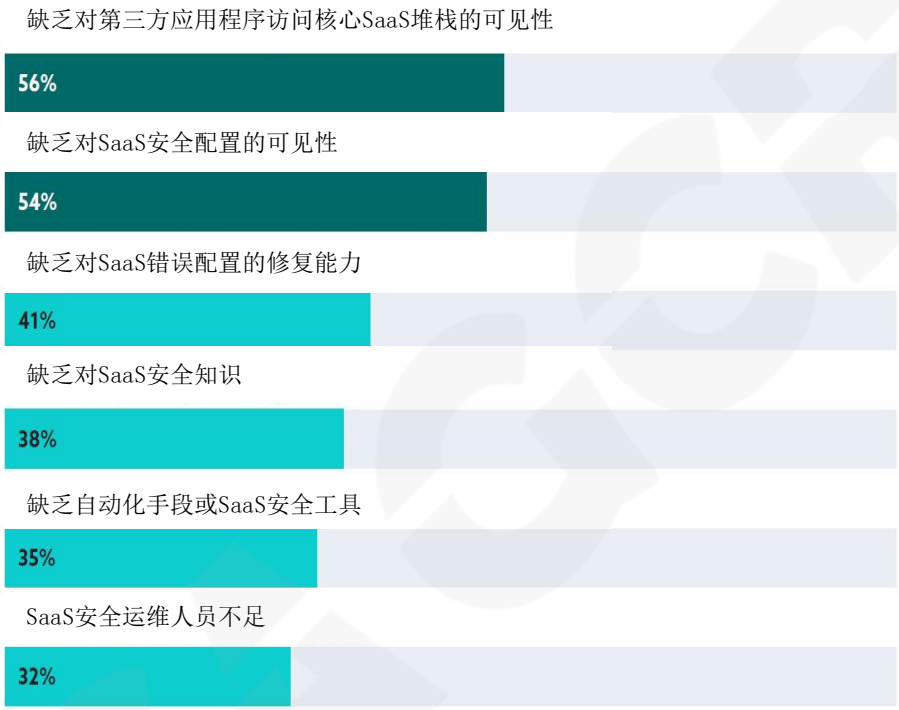


近年来企业在SaaS应用程序及安全上的投入变化

尽管在过去的一年中，许多企业改变了他们对SaaS应用程序和安全性的投入策略，然而，在核心业务相关的SaaS应用程序的投入仍然超过了在安全运维工具及人力上的投入。如果这一趋势持续下去，企业安全运维团队的负担将持续加大。

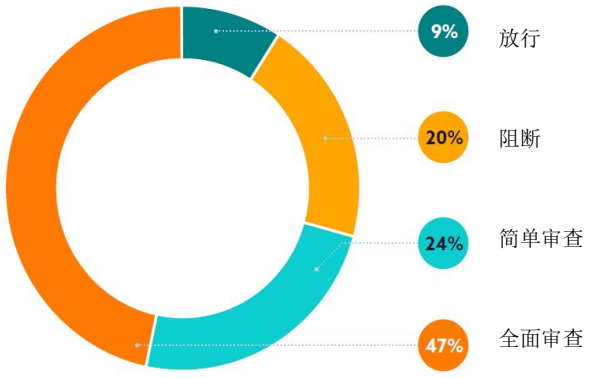
第三方应用程序访问是企业部署SaaS应用程序时的最大关注点

企业在部署某个SaaS应用程序时最担心的是缺乏对应用程序的可见性，确切的说，他们担心的是缺乏对那些能够访问企业核心SaaS堆栈（56%）和安全配置（54%）的第三方应用程序的可见性。最不担心的则是SaaS安全运维人员的不足（32%），这能够解释之前企业在安全运维人员上的投入不足。



企业发现未经许可的SaaS应用时的应对策略

当发现未经许可的SaaS应用时，47%的企业会进行全面的安全策略审查，大约1/4的企业（24%）会进行简单、快速的安全审查。



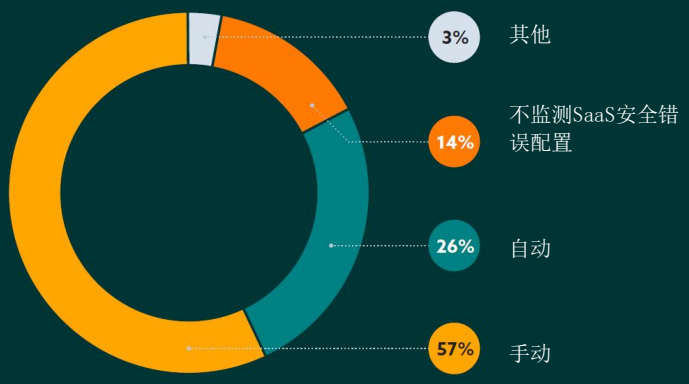
Saas安全评估

谁负责SaaS应用程序的安全设置

通常，负责Saas应用程序安全设置的部门不限于IT部门或者安全部门。占比最高的部门分别是安全部门（59%），IT部门（50%）和业务部门（40%），意味着多个部门置身安全之外。虽然业务应用程序所有者有充分的理由拥有相应级别的访问权限，但是这些部门缺乏正确的安全知识，也缺乏对维护应用程序安全性的兴趣，最终会给安全部门和IT部门带来问题。

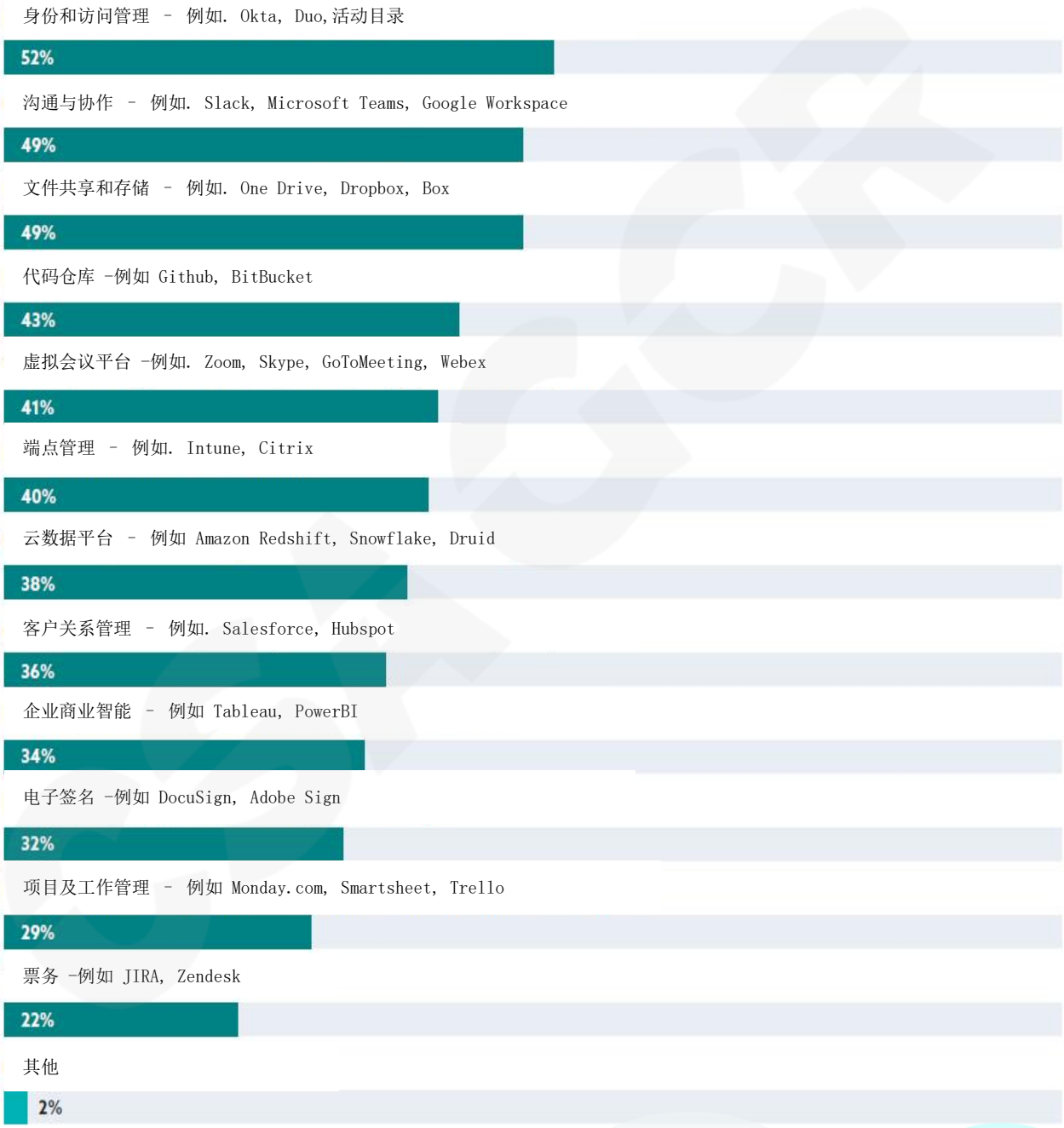
监测Saas安全配置的方法

监测SaaS安全配置的最常见方法是手动(57%)。在那些采用手动监测的组织中，大约63%手动执行此评估。这种方法不仅耗时，而且容易出现人为失误。每七个组织中就有一个根本没有监测Saas安全，原因可能有很多，其中之一可能是缺少资源（例如，缺少自动化监测工具，缺乏手动监测人员）。



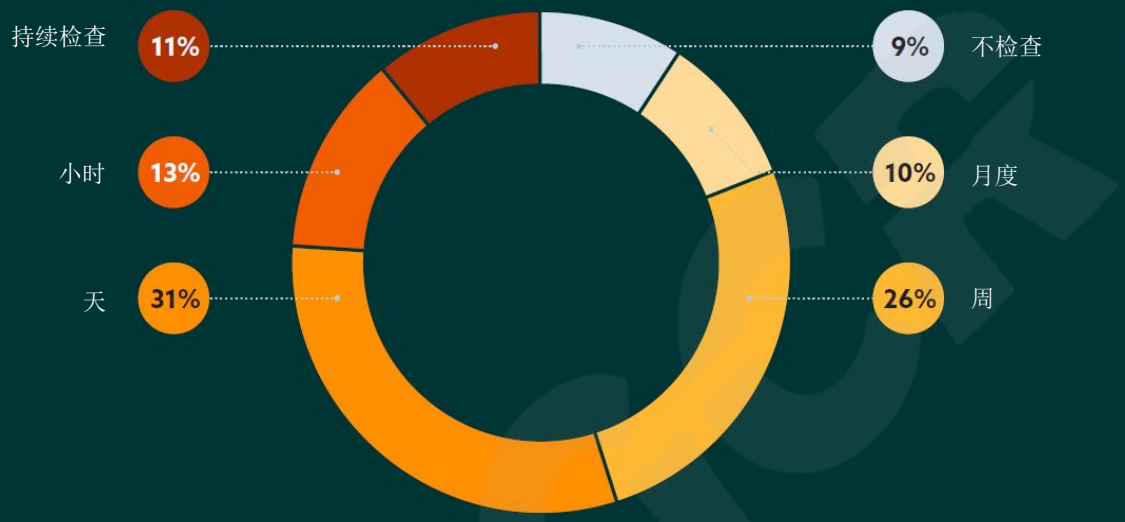
应用程序错误配置评估

组织监视各种SaaS应用程序的错误配置。最受关注的应用程序是IAM（52%），通信和协作平台（49%），文件共享/存储（49%）。尽管关注点之间存在微小的差异，但很明显，组织对其整个SaaS应用程序堆栈感到担忧。



SaaS安全配置评估时长

三分之一的组织需要超过一周的时间评估SaaS安全配置。这就解释了为什么一些组织没有监测他们的SaaS安全配置，这是一个非常消耗时间和资源的过程。



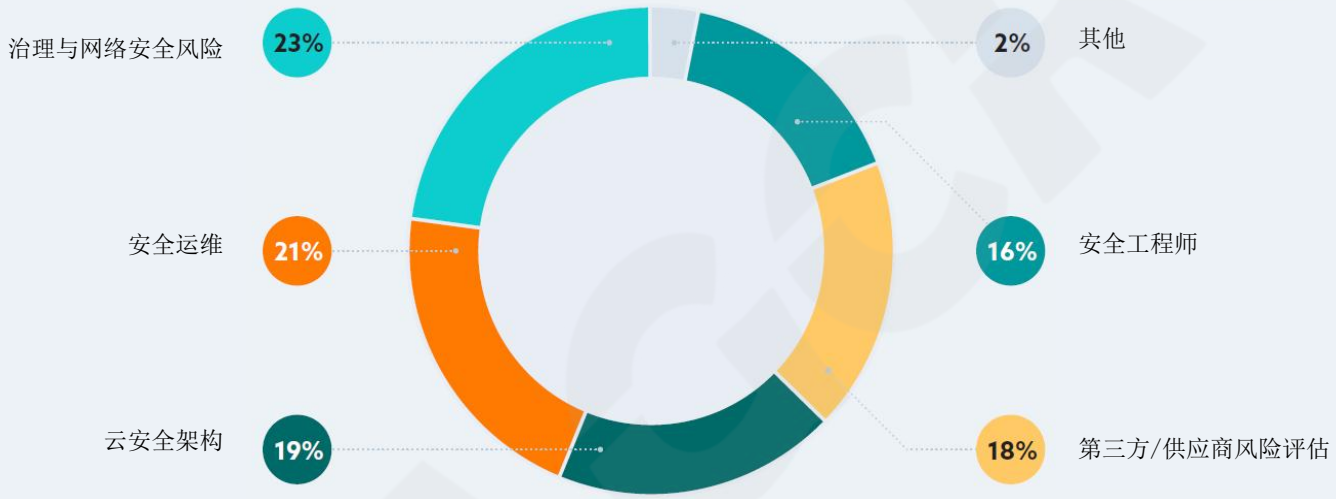
SaaS安全配置评估频率

40%的组织每月或更低的频率检查其SaaS安全配置，十分之一的组织每年才检查一次，而最常见的是每周一次（23%）。

SaaS安全的错误配置

谁负责SaaS安全错误配置的检测和修复

负责检测和修复SaaS安全错误配置根据组织的不同而不同。最常见的反应是治理与网络安全风险(23%)和安全运维(21%)。

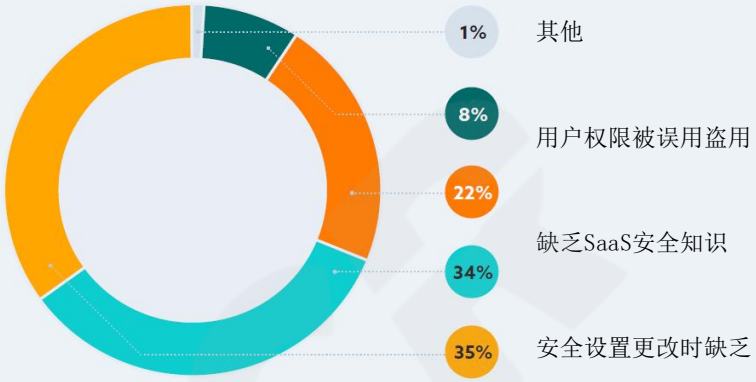


与SaaS安全错误配置相关最值得关注的领域

组织最担心的与SaaS安全错误配置相关的领域是数据防泄漏(55%)、访问控制、密码管理和多因素认证(54%)。这些问题相互关联，组织希望避免未授权访问和泄漏公司的重要数据。

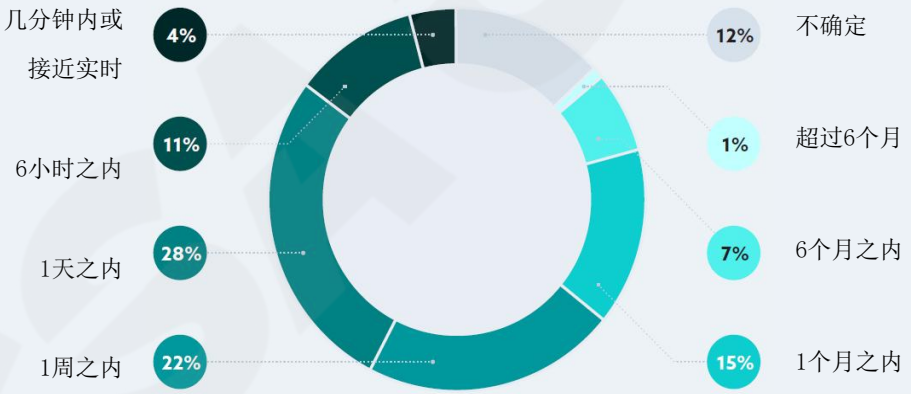
造成SaaS错误配置的主要原因

造成SaaS错误配置的两个主要原因是，有太多业务部门可以访问SaaS的安全设置（35%），以及配置变更时缺乏可见性（34%）。负责检测和修复SaaS错误配置的安全团队需要深入了解设置的变更，尤其是在其他业务部门可以访问的情况下。有了这种洞察力，安全团队可以快速与其他业务部门合作，修复错误配置或防止其发生。



修复SaaS安全配置错误的时间

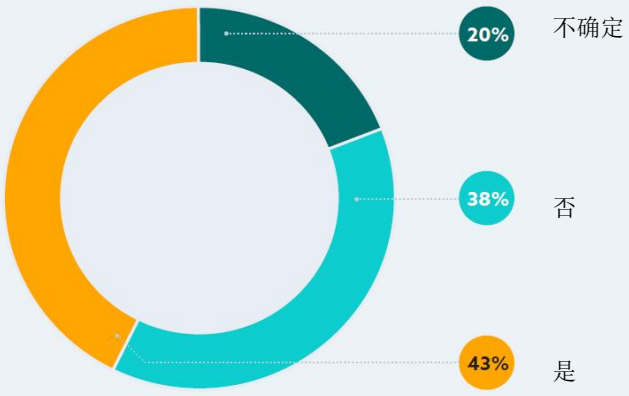
对于大多数组织来说，修复错误配置大约需要一天（28%）或一周（22%）；同时，几乎相同数量比例的组织需要一个月或更长时间（23%）。然而，对于SSPM用户来说，时间缩短了。近3/4使用SSPM的组织可以在一天内解决错误配置。



过去一年中由于SaaS安全错误配置导致的安全事件

降低检测和修复SaaS安全错误配置的时间，对防止SaaS安全事件至关重要。然而，43%的组织由于错误配置导致安全事件发生。

同时，由于SaaS用户数量不确定，这一比例可能高达63%。



SaaS安全工具

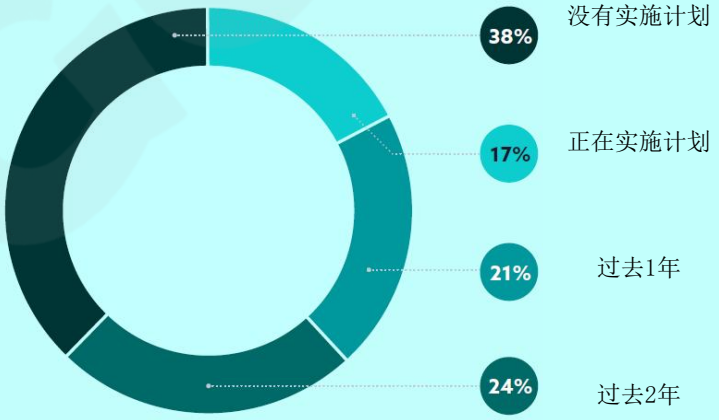
对云安全解决方案及其优势的熟悉程度

我们调查评估了SaaS使用者对四种云安全解决方案的熟悉程度。有趣的是，SSPM的平均评分为“有点熟悉”；尽管SSPM市场在大约两年前才推出，但它似乎正在迅速成熟。

SSPM的使用情况与计划

计划或目前已经在使用SSPM的组织，占比为62%，也表明了SSPM在市场上的迅速采用和成熟。同时，计划实施SSPM的最常见原因是能够检测和自动修复SaaS错误配置（54%）以及SaaS应用程序中对违反策略的可见性（23%）已经使用SSPM的组织认为，他们的SaaS安全性得到了改善（51%），并通过SaaS安全管理和维护节省了时间（33%）。

只有38%的组织目前没有实施SSPM的计划。不计划实施SSPM的最常见原因是不熟悉（46%）和缺乏实施新解决方案的资源（25%）。



结论

组织可以提升SaaS安全的关键方法：

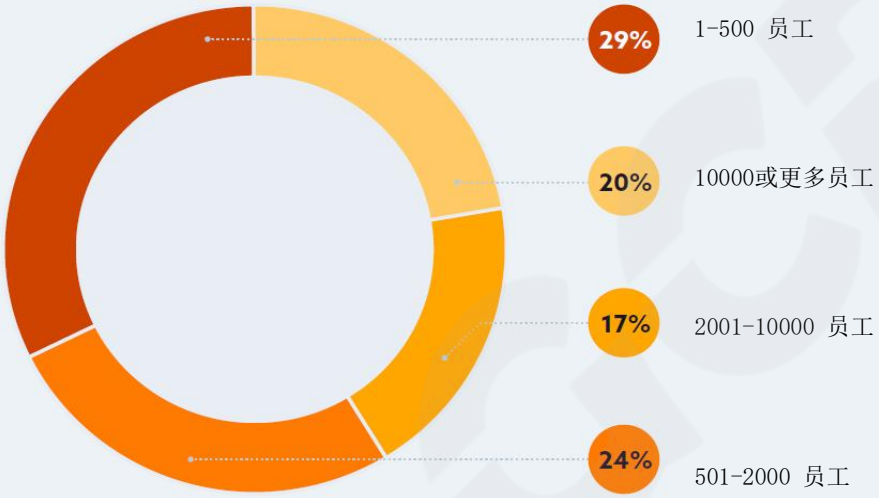
1. 为安全团队提供对SaaS应用程序安全设置可见性的能力，包括第三方应用程序访问和用户权限的配置情况。这种可视性允许多个部门保持其访问权限，而不会导致不适当的变更，从而使组织免受攻击。
2. 利用自动化工具监控和修复SaaS安全错误配置，如SSPM。自动化使安全团队能够近实时地解决这些问题，减少组织易受攻击的时间，或防止发生安全事件。

这些措施为组织的安全团队提供支持，同时不妨碍其他部门继续工作，从而避免重大安全事件。

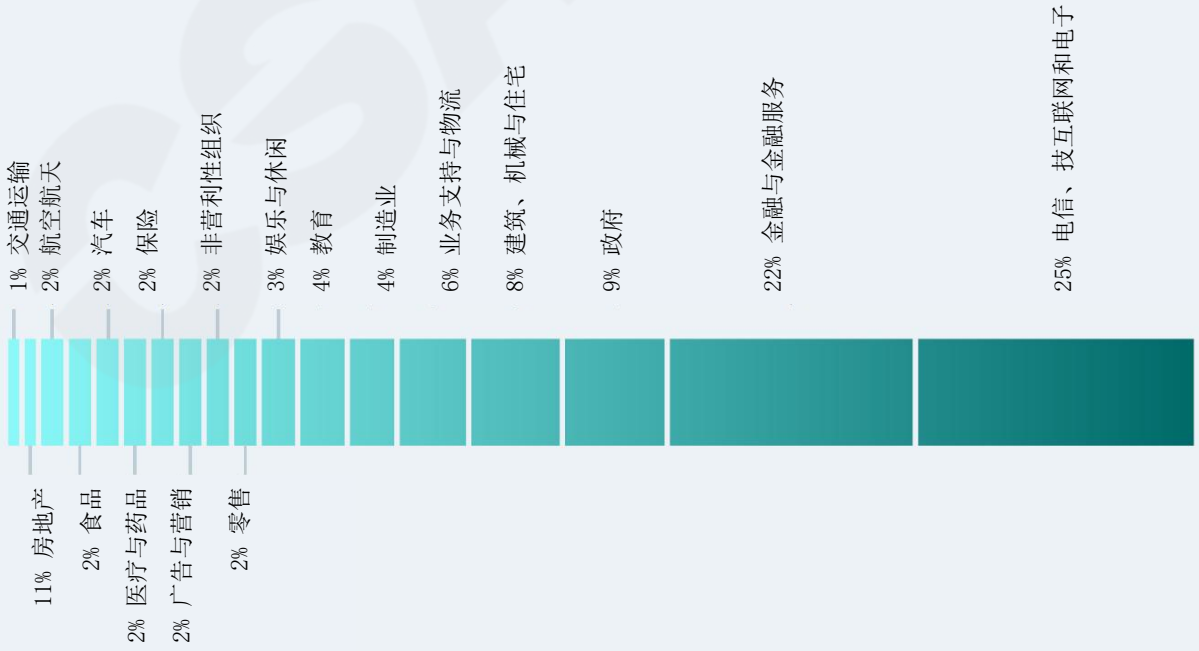
统计结果

本次调查在2022年1月至2月进行，一共收集了340份来自不同规模、行业、地区和角色的IT和安全专业人员的答卷。

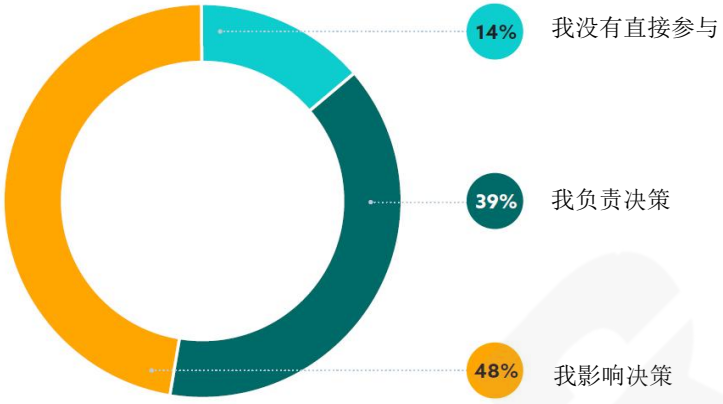
贵公司的规模大小?



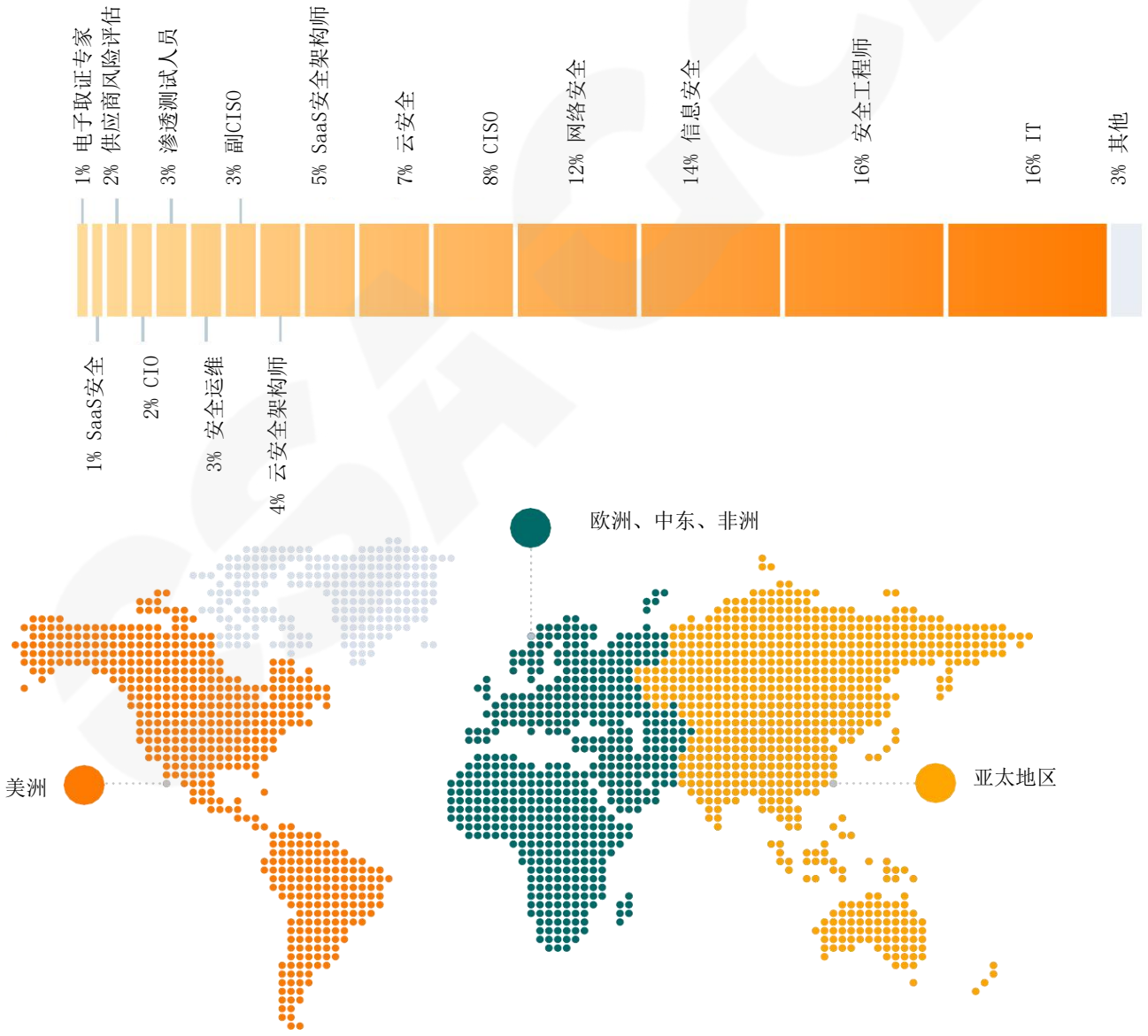
贵公司所属行业?



您在引入新战略的决策过程中属于什么角色?



以下哪项最符合你的岗位?



本报告赞助方

领先的SaaS安全态势管理（SSPM）公司Adaptive Shield，使安全团队能够快速发现并修复其SaaS环境中的错误配置，确保符合公司和行业标准。Adaptive Shield与众多财富500强企业合作，帮助它们控制SaaS威胁。

有关更多信息，请访问www.adaptive-shield。com或在LinkedIn上关注我们。

ADAPTIVE SHIELD