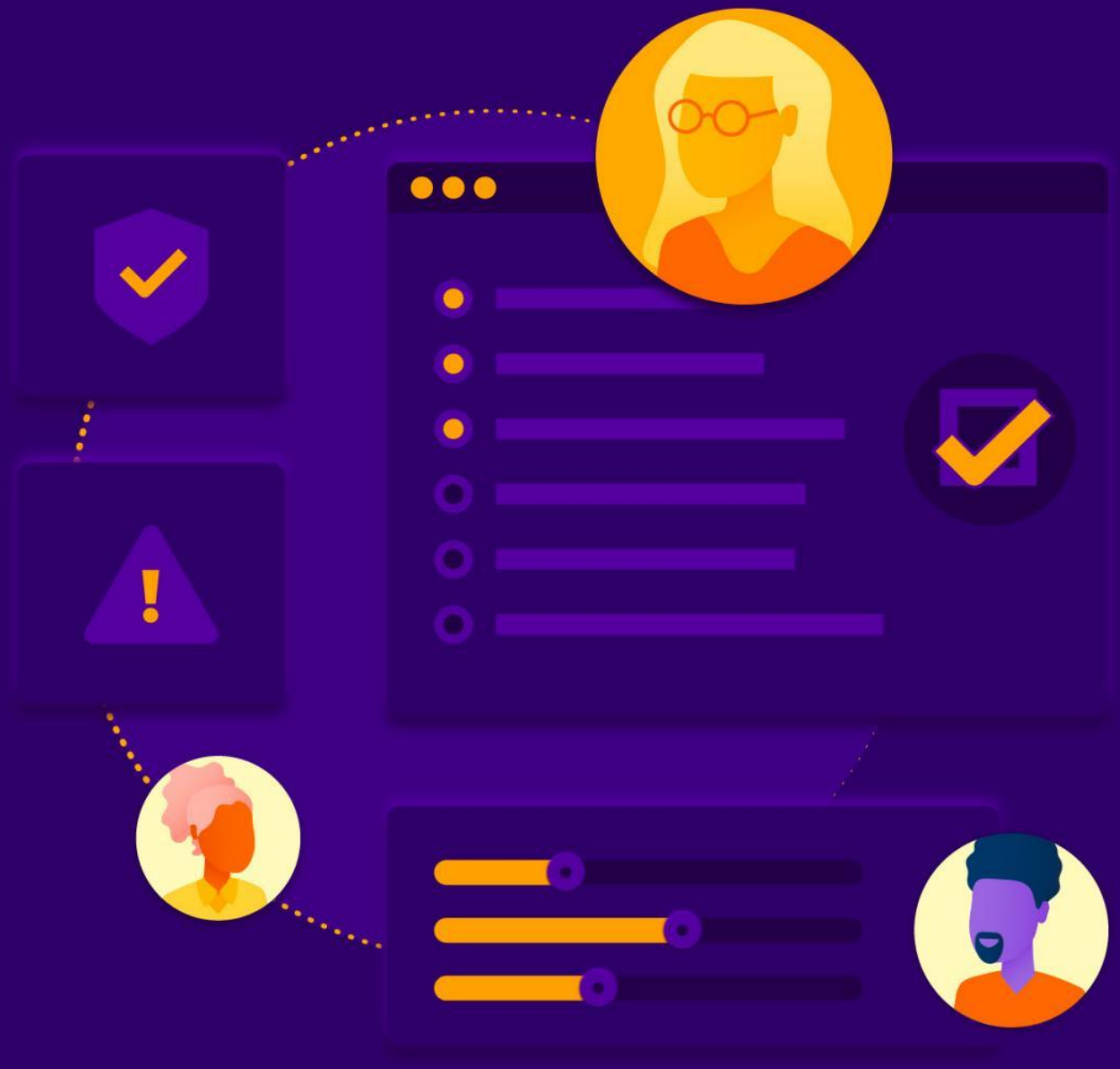
洞察2022

云上数据安全与重要事项



CSA GCR cloud security alliance GREATER CHINA REGION

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

《洞察 2022-云上数据安全与重要事项（Understanding Cloud Data Security and Priorities in 2022）》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：

黄鹏华　　鹿淑煜　　陶瑞岩　　王彪　　薛琨　　余晓光

审校组：

郭鹏程　　王阳　　王亮　　顾伟

感谢以下单位的支持与贡献：

安易科技（北京）有限公司　　北京天融信网络安全技术有限公司

北森云计算有限公司　　华为技术有限公司

三未信安科技股份有限公司　　上海安几科技有限公司

英文版本编写专家

主要作者：Hillary Baron

贡献者：

Josh Buker　　Sean Heide　　Alex Kaluza　　John Yeoh

设计师：Claire Lehnert

特别鸣谢：Neil Patel

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。

序言

《洞察 2022-云上数据安全与重要事项》（Understanding Cloud Data Security and Priorities in 2022）调查报告由 CSA 工作组专家编写，CSA 大中华区秘书处组织翻译并审校。报告的主要内容是关于云上数据安全和重要事项的洞察和建议。它包括了对云安全现状的分析、云安全风险的评估、云安全最佳实践的介绍以及未来云安全发展趋势的预测。通过报告，组织可以了解到如何加强自身能力、控制第三方访问权限、管理暗数据、定期进行漏洞扫描和安全评估、加强员工安全意识培训以及选择可信赖的云服务提供商等方面来保护其云上敏感数据。这些建议和最佳实践将帮助组织更好地应对当前和未来的云安全挑战，确保其数据在云上得到充分的保护。

CSA 于 2022 年 7 月通过线上开展这项调查，收到了 1633 份回复，分别来自于不同规模、不同地点组织内的信息技术和安全专业人员。CSA 的研究分析师对这份报告进行了数据分析和说明，阐述了 4 个重要发现，重要发现 1：各组织正在努力保护和跟踪云中的敏感数据；重要发现 2：第三方和供应商对敏感数据的访问权限相似；重要发现 3：暗数据问题源于人员配置问题和部门间的冲突；重要发现 4：大多数安全专业人士认为，他们的企业明年将会遭遇数据泄露。此调查报告总结详尽，数据分析维度值得大家参考。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

调查的创建和方法

云安全联盟(CSA)是一个以广泛推广在云计算和IT技术领域保障网络安全最佳实践为使命的非营利性组织。CSA还向行业中利益相关者们针对各类其他计算形式的安全问题提供教育。CSA会员是由行业从业者、企业和各专业团体所组成的多领域联盟。CSA的主要目标之一是开展评估信息安全趋势的调查，这些调查提供了有关组织当前在信息安全和技术方面的成熟度、意见、兴趣和意图等信息。

BigID委托CSA进行了一项调查和报告，以便更好地了解业界对云数据安全的认知、态度和意见。BigID资助该项目并联合CSA研究分析师共同制定了调查问卷。CSA于2022年7月通过线上开展这项调查，收到了1633份回复，分别来自于不同规模、不同地点组织内的信息技术和安全专业人员。CSA的研究分析师对这份报告进行了数据分析和说明。

研究目标

本研究目标是理解以下内容：

- 实现云数据安全的方法
- 云数据安全的优先事项
- 敏感数据和暗数据的当前状态
- 对数据泄露的担忧
- 法律合规的困难

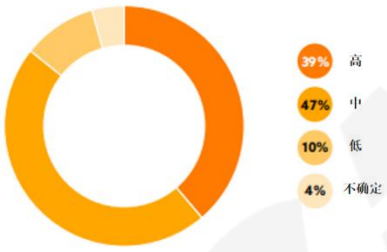
重要发现

重要发现1：

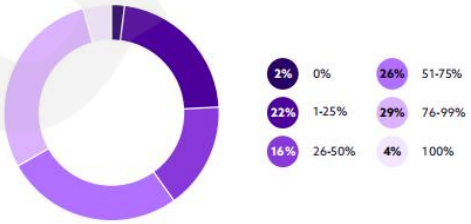
各组织正在努力保护和跟踪云上的敏感数据

总体而言，组织对其在云上保护数据的能力缺乏信心，报告显示，39%的组织有较高的信心。超过一半的组织(57%)表示其信心处于中等至较低水平。当讨论敏感数据时，明显更加缺乏信心。40%的组织表示，他们在云上的敏感数据只有50%或更少具有足够的安全性。只有4%的组织表示，他们在云端的所有数据具有足够的安全保障。这一发现表明，组织通常对自己保护数据的能力有一定的信心，但在涉及敏感数据时却举步维艰。

组织在云上保护数据能力的信心度



在您看来，您的组织中有多少敏感数据是在云上得到了充分保护的？



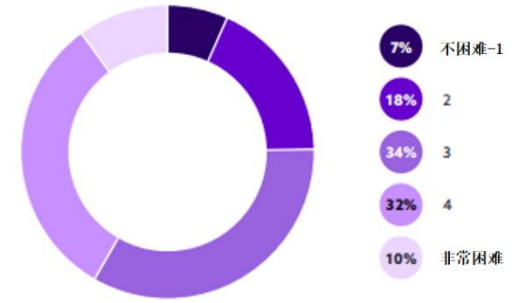
除了努力保护敏感数据，组织还在努力跟踪云上的数据。超过四分之一的组织没有跟踪受监管的数据，近三分之一的组织没有跟踪机密数据或内部数据，45%的组织没有跟踪未分类数据。这表明，组织目前对数据进行分类的方法不足以满足他们的需求。

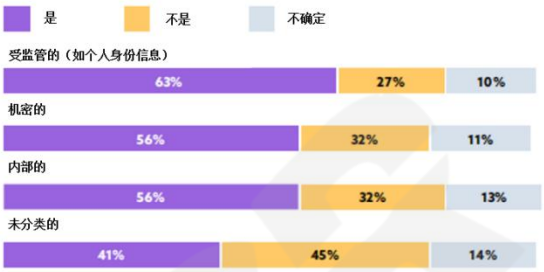
对于SaaS平台，76%的组织将跟踪数据的困难级别评为中级到高级。只有7%的组织表示跟踪数据根本不是问题。当考虑到组织在SaaS平台中拥有的敏感数据量时，数据跟踪的难度尤其令人担忧。

这些数据跟踪方面的难题可能与缺乏使用数据分类和发现机制有关，只有9%的组织使用这些功能。以上功能缺乏可能与缺乏能力（52%）和缺乏跨平台支持（41%）有关，这些都是需要选择第三方云数据安全供应商的原因。无论如何，使用数据分类和发现机制将使组织

能够更好地跟踪其数据。

SaaS 平台中跟踪数据的难度构成级别　　云上被跟踪的数据





重要发现2：

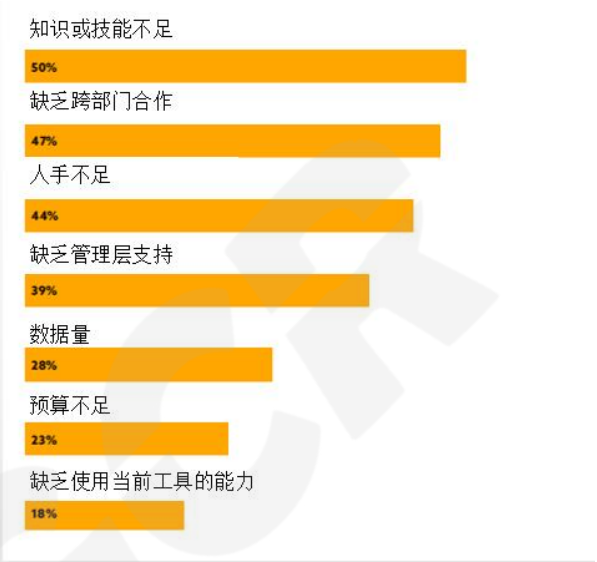
第三方和供应商对敏感数据的访问权限与员工权限相似。

组织似乎向员工、承包商、合作伙伴和供应商提供了几乎相同级别的敏感数据访问权限。这一发现表明，第三方和供应商可能对组织的敏感数据有过多的访问权限，尤其是考虑到最近热门的供应链攻击。在CSA最近的一份关于云和网络攻击的调查报告中发现，第三方、承包商和合作伙伴是攻击中最常见的目标群体（58%）。此外，根据科罗拉多州立大学的一项研究，2/3的违规行为是由供应商和第三方漏洞造成的。考虑到这些影响的严重性，组织需要了解谁有权访问其敏感数据，并锁定访问权限，特别是第三方的访问权限。

重要发现3：

暗数据问题源于人员配置问题和部门间的冲突

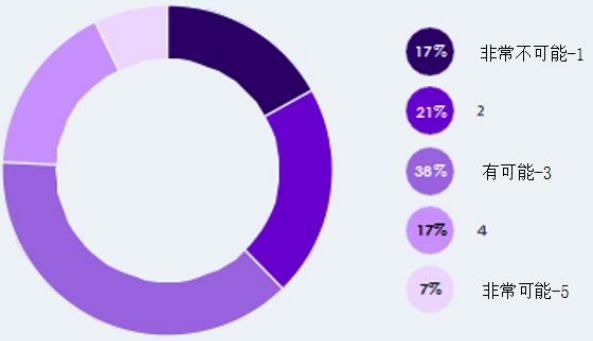
超过一半的组织(79%)对其组织中的暗数据扩散有中度到高度的担忧，但不确定如何解决这一问题。组织获取暗数据的三大障碍与人员配置有关：技能和知识的不足(50%)、缺乏跨部门合作(47%)和人力资源不足(44%)。组织需要致力于培训员工，并优先考虑能够弥补人员缺口的技术。此外，组织需定义一种统一的方法来处理暗数据，以避免孤立部门的优先事项相互竞争。建立单一的数据源（例如数据清单）可以为不同的部门提供他们所需的基础知识，以便他们更紧密地工作



重要发现4：

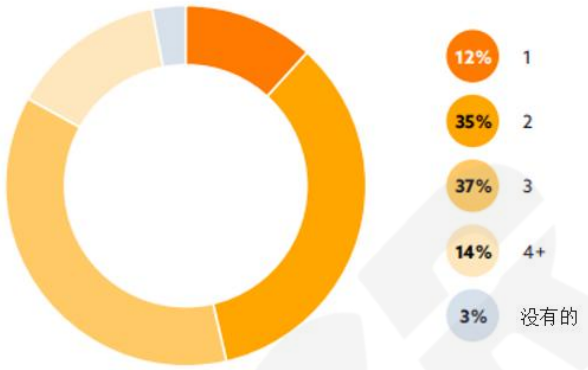
大多数安全专业人士认为，他们的企业明年将会遭遇数据泄露。

62% 的组织称他们在未来一年某种程度上极有可能遭遇云数据泄露。鉴于在过去的12个月里有大量的组织遭遇过云数据泄露事件，人们对未来12个月发生的未遂泄露有更大的担忧是有道理的。对于过去12个月没有遭遇过入侵的组织，22%的受访者表示，未来12个月发生入侵的可能性非常小。经历过数据泄露的组织认为，数据泄露的可能性更大，只有8%发生过泄密的组织受访者表示未来12个月内发生数据泄露的可能性很小。组织的一个关键步骤是锁定第三方对敏感数据的访问。组织还需要继续为其复杂的云环境(例如多云和混合云)确定跨平台支持的优先顺序，以确保所有环境的安全性。



概述

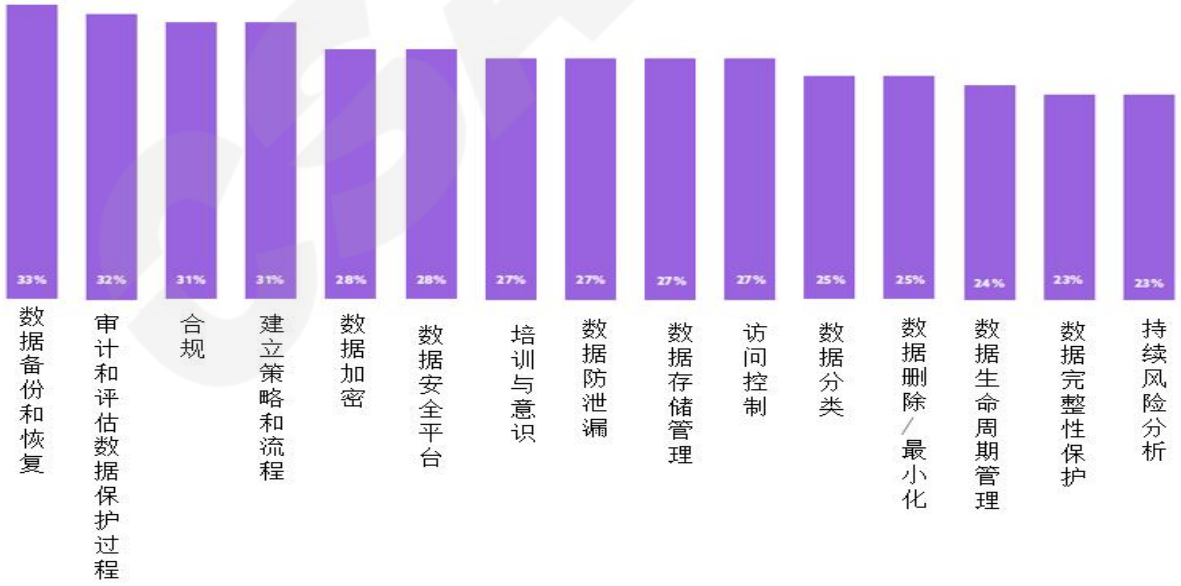
用于数据存储的IaaS和PaaS平台数量



绝大多数(86%)的组织利用多个云平台存储数据。大多数组织使用2个 (35%)或3个(37%) IaaS或PaaS云平台来存储数据。只有12%的组织使用了1个云平台。

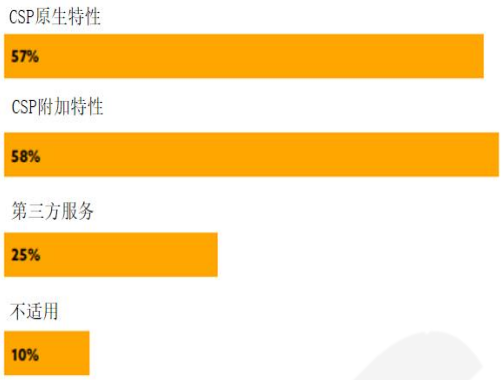
数据保护策略

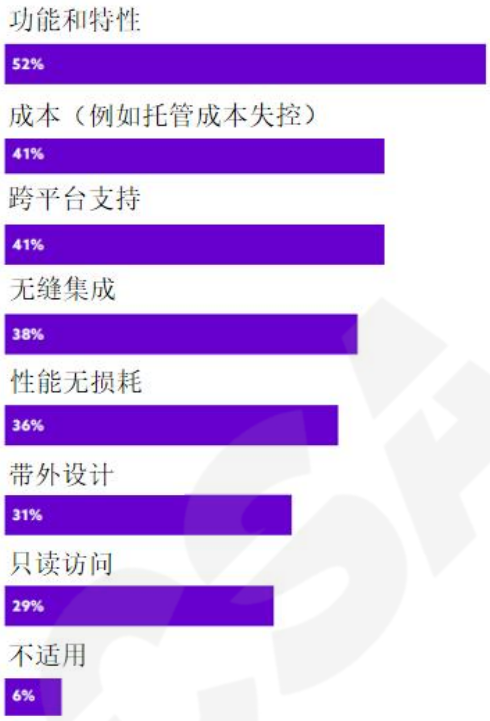
组织在其数据保护策略中通常使用4到5个不同的组件。一些最常见的组件包括数据备份和恢复(33%)、审计和评估数据保护过程(32%)、遵守标准和监管合规(31%)以及建立策略和流程(31%)。一些不太常用的组件包括分类告警(18%)、零信任(19%)和数据主权(19%)。看起来尽管是在朝着零信任的方向发展，但许多组织的数据保护尚未完全整合。



云数据安全使用的服务类型

组织主要依靠云服务提供商的功能，无论是原生功能（57%）还是附加功能（58%）。只有四分之一的组织使用了第三方服务。





选择第三方云数据安全供应商的驱动力

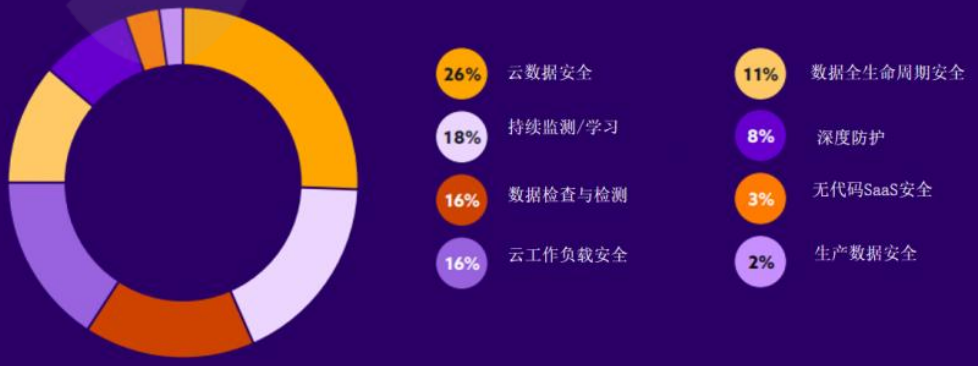
对于使用第三方服务实现云数据安全的组织来说，他们选择供应商时考虑的前三个因素是功能和特性（52%）、成本（41%）和跨平台支持（41%）。这表明，选择第三方服务的组织正在寻找更具成本效益或电信运营商不能够提供的附加功能。此外，多云和混合云环境的应用使组织关注于跨平台支持。

应用的数据安全功能

组织使用的最常见的数据安全功能是持续监测/学习（48%）、云工作负载安全（42%）、云数据安全（42%）以及数据检查和检测（41%）。有趣的是，最少利用到的数据安全功能是数据发现和数据分类。数据发现及数据分类使用率低的原因可能是因为组织认为数据发现和数据分类是数据安全生命周期的一部分。然而，使用率如此之低，这可能是导致暗数据问题的一个因素。组织需要利用数据发现和数据分类工具来正确理解他们拥有的数据以及如何保护这些数据，否则数据将继续成为暗数据。

高优先级数据安全产品功能

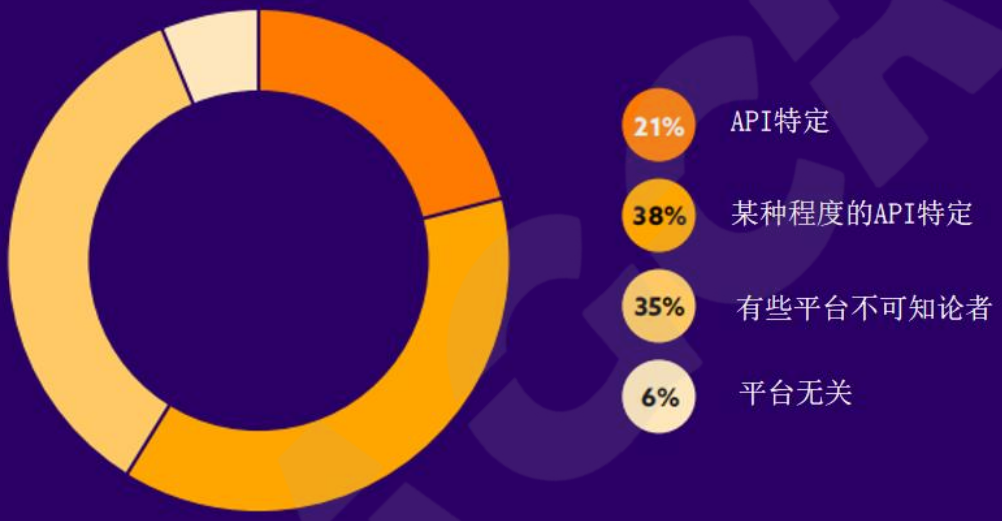
在组织使用的数据安全功能中，最优先的功能是云数据安全（26%）、持续监控/学习（18%）、数据检查和检测（16%）以及云工作负载安全（16%）。这些结果遵循与组织通常使用的数据安全特性类似的模式。



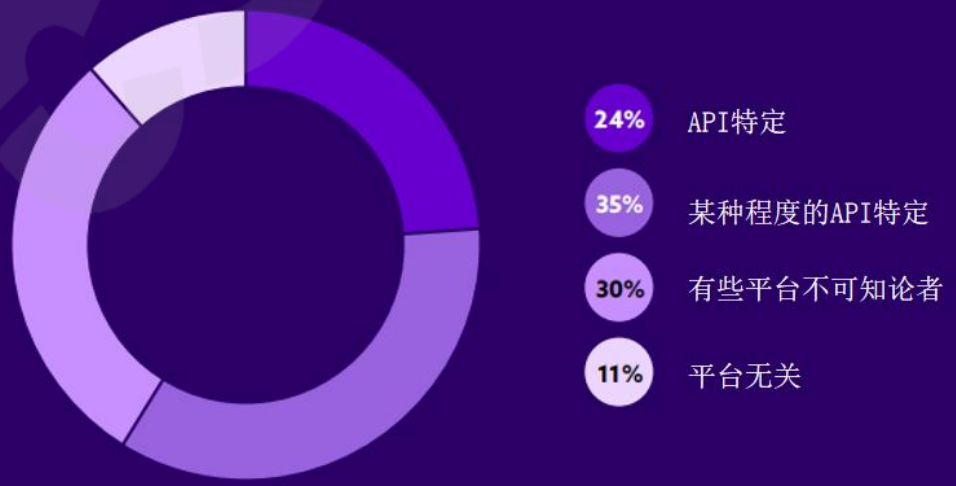
当前的数据互操作性方法

总体而言，组织倾向于采用特定API的方法（59%）来实现数据互操作性，而不是平台无关（41%）。组织似乎对他们的方法感到满意。当被问及数据互操作性的理想方法时，回答基本相同，组织大都倾向于API特定的方法（59%），而不是平台无关的方法（41%）。组织需要能够轻松集成其当前解决方案并利用开放API的工具。

数据互操作性的当前方法



组织数据互操作性的理想方法

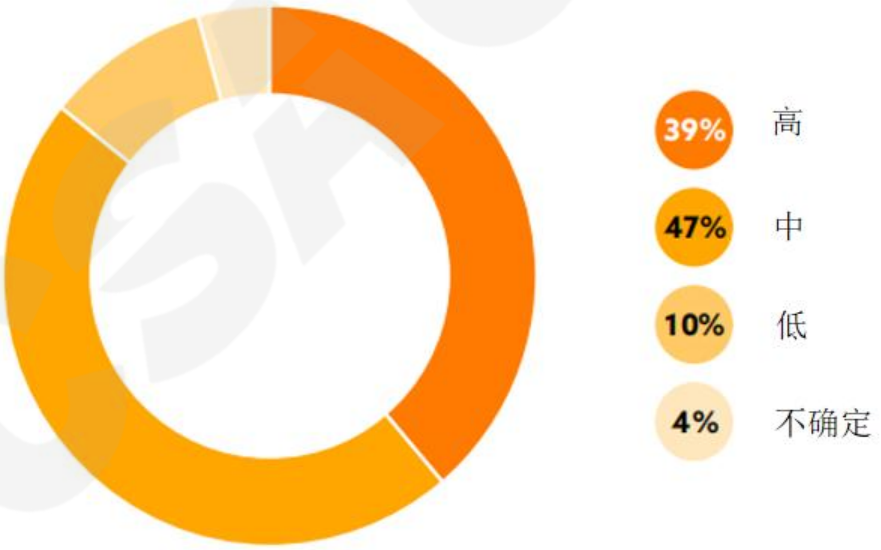


敏感数据

对保护云上数据能力的信心

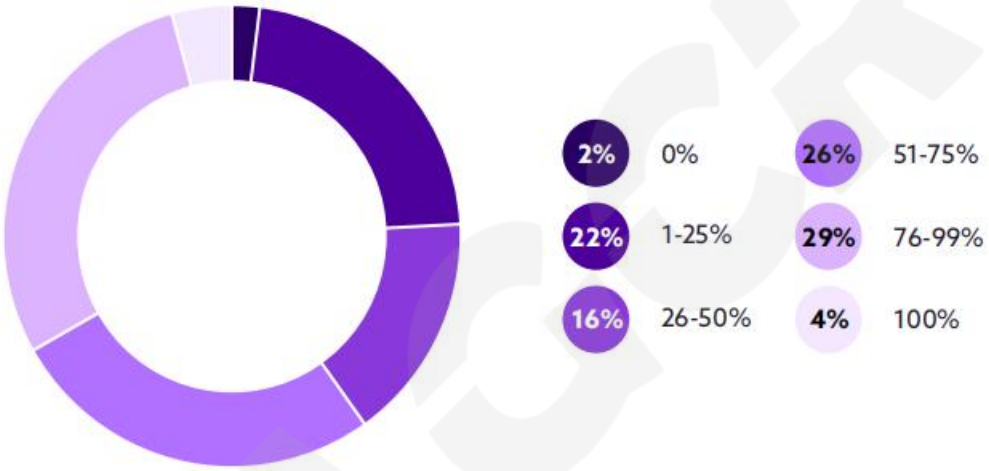
组织对他们保护云上数据的能力充满信心，39%组织高度自信，47%组织中度自信。虽然这些结果看起来令人鼓舞，理想情况下，大多数组织应该对其自身的能力感到高度自信。目前大多组织仅为中度自信的事实表明，组织的云上数据安全策略还有很大的改进空间。

值得注意的是，组织的信心也受近期发生的数据泄露事件和受访者在组织的地位的影响。对于在过去一年中发生过数据泄露的组织，他们的信心会下降。在那些对自己保护云上数据的能力有高度信心的受访者中，36%在过去一年中发生过数据泄漏事件，40%没有发生数据泄漏事件。最近没有发生过数据泄露的组织，可能对自己保护云上数据的能力过于自信，直到自己亲身经历了数据泄露。此外，经理(40%)选择高度自信的比例高于高管(35%)和员工(34%)。



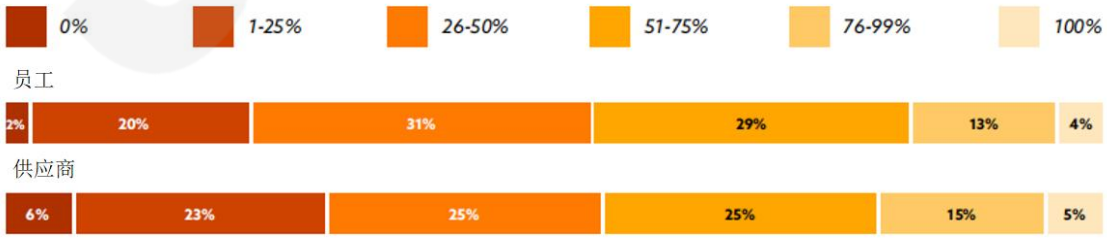
云上敏感数据具有足够安全性的比例分布

40%的组织表示，他们在云上的敏感数据有足够安全性的不超过50%。只有4%表示，他们云上数据100%有足够的安全性。这也意味着96%的组织至少在敏感数据上没有足够安全性保障。这些数字相当震惊。这可能导致组织对自己保护云上数据的能力缺乏信心，或者意味着组织对其保护数据的能力过度自信。



可访问敏感数据的员工比例分布

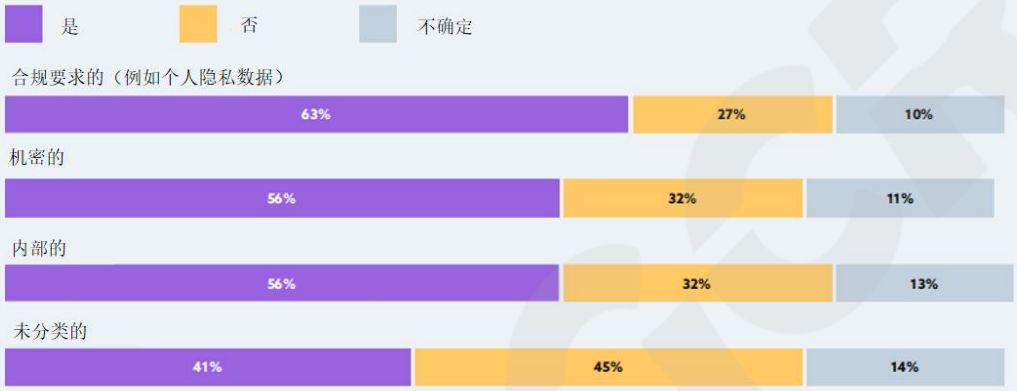
组织给予员工和供应商对敏感数据几乎相同级别的访问权限。特别结合最近热门的供应链攻击事件，表明第三方合作伙伴和供应商对组织敏感数据有过高的访问权限。组织应该敏锐地掌握谁可以访问以及他们可以访问什么，以防止无意识的信息泄漏。



暗数据

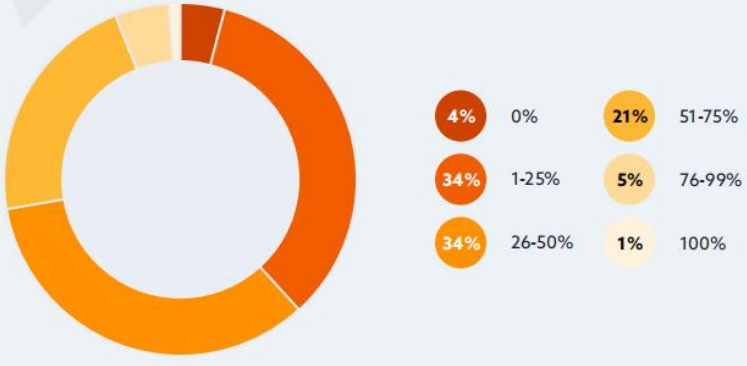
追踪云上数据

组织正在努力追踪云上数据。超过四分之一的组织没有对受监管的数据进行追踪，近三分之一的组织没有对机密的或内部数据进行追踪，45%的组织没有对未分类数据进行追踪。这表明，组织目前的数据分类方法不能满足他们的需求。



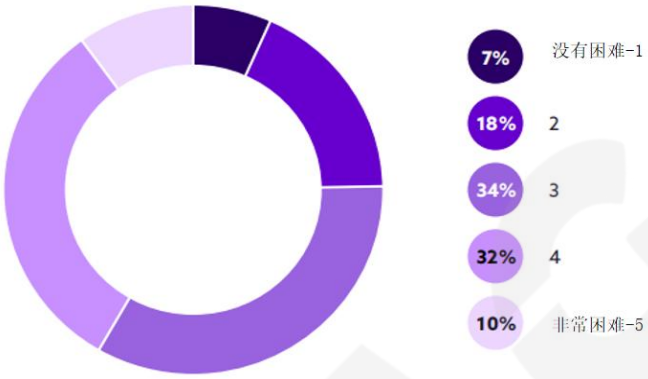
暗数据百分比

诚然，如果没有合适的工具，很难评估组织所拥有的暗数据数量。然而，当需要进行评估时，超过四分之一（27%）的安全和技术专业人士认为，他们组织的数据中有51%或更多是暗数据。虽然这个比例高的惊人，但实际数量可能更高。这也表明安全专业人员意识到存在问题，但难以理解问题的严重程度。这是一个严峻的问题，如果组织对数据以及其存放位置不具有适当的可见性，就无法保护数据。如果不解决暗数据的问题，组织就无法正确了解数据风险状况或者评估存在的攻击面，这会导致漏洞和安全问题。



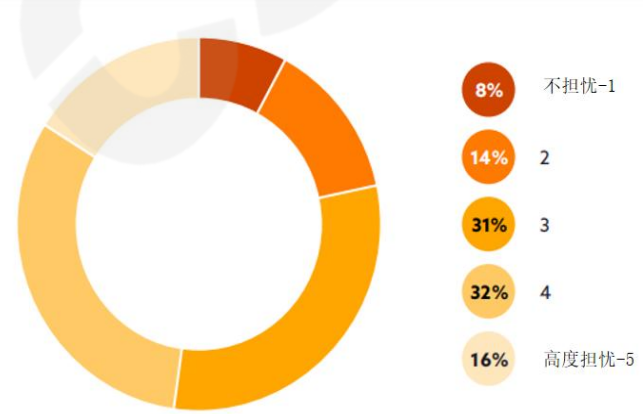
SaaS平台追踪数据的难度等级

组织努力在SaaS平台中进行数据追踪。76%的组织认为这对他们的组织来说是比较甚至极其困难的。只有7%的组织表示这点对他们来说完全没有困难。这些困难可能是由于缺乏可见性、输入的数据量大，甚至缺乏合适的工具。许多组织(91%)表示没有使用数据分类或发现工具，这可能是造成此问题的原因之一。有可能是由于当前工具中缺乏相关功能(例如，它们无法为组织提供对SaaS应用程序中的敏感数据的可视化)。组织需要持续强调他们对第三方数据安全供应商的跨平台支持，以确保覆盖范围扩展到到他们整个数据生态系统，特别是SaaS平台。



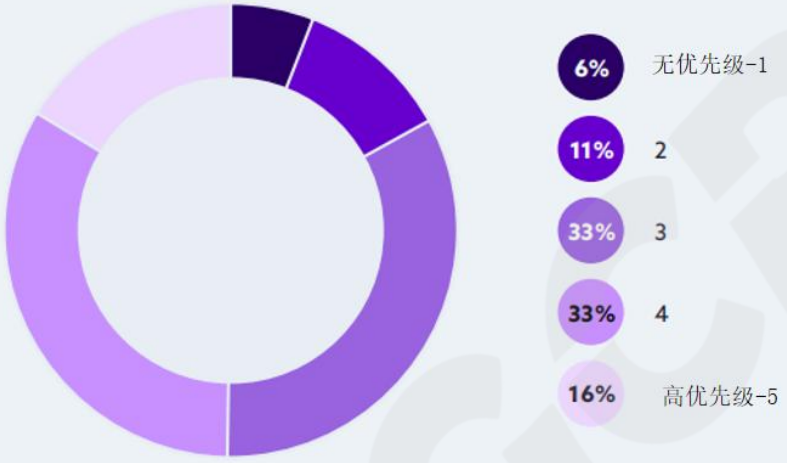
对暗数据扩散的担忧程度

近一半（48%）的组织高度关注其组织中暗数据的激增。鉴于目前缺乏对其追踪以及在SaaS平台中追踪数据的难度，组织尚不清楚如何解决这个问题。很明显，组织在数据资产管理方面举步维艰，并且缺乏完整的数据可见性和控制手段。



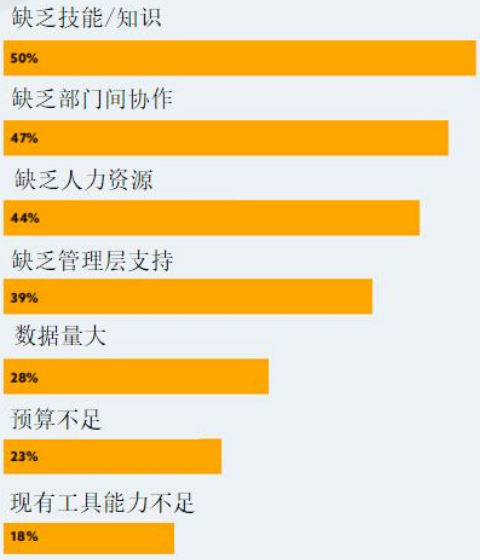
捕获暗数据的优先级

尽管存在困难，但组织对暗数据的担忧促使他们优先捕获暗数据。82%的组织表示这是中到高优先级的工作。组织似乎了解暗数据给其组织带来的安全、隐私和合规风险、成本和竞争劣势，更多的组织需要考虑使用数据发现工具来遏制暗数据问题。



捕获暗数据的首要障碍

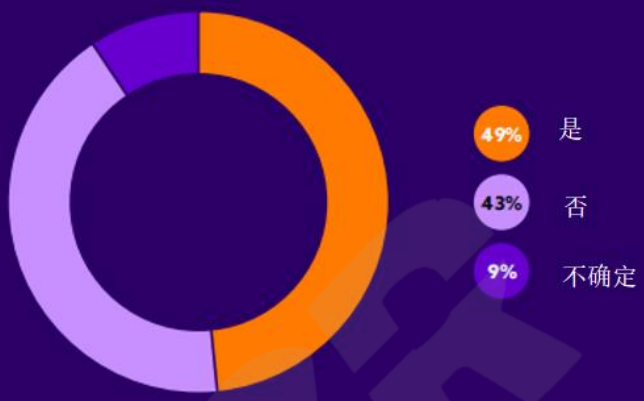
组织捕获暗数据的三大障碍与人员配备直接相关：缺乏技能/知识（50%）、缺乏部门间合作（47%）和缺乏人手（44%）。组织需要致力于培训他们员工，优先考虑可以弥补人员缺口的技术。还需要利用自动化、机器学习或人工智能工具，帮助增加团队的知识/技能，并补充现有人员缺口。组织还应该建立统一的平台，以供各部门合作，提供团队协同工作所需要的统一基础知识。



数据泄露

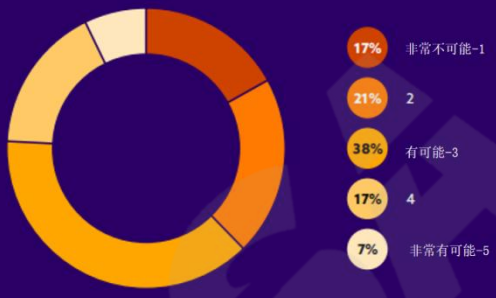
过去12个月的云上数据泄露

近一半 (49%)的组织表示过去12个月发生过云上数据泄露事件。考虑到他们对保护云上数据能力的高度自信，现实情况似乎更加严峻。这可能是由于组织使用云环境越来越复杂，使得制定通用数据安全战略更加困难。



在未来12个月，发生云上数据泄露的可能性

62%的组织认为云数据泄露的可能性较高。鉴于在过去12个月经历过云上数据泄露的组织数量众多，预计未来12个月会有更多人对企图泄露数据的行为感到担忧。对在过去12个月发生过数据泄漏的组织来说，他们普遍认为 “有可能”对没有发生过数据泄漏的组织，他们的反应介于“非常不可能”和“有可能”之间



数据泄露的影响

数据泄露对组织最大的影响是财务方面。这很可能是因为所有潜在的影响如法律、声誉和运营停滞，最终都会归结为罚款、服务成本或工作损失给组织带来的成本。运营停滞带来影响的平均排名明显更低。这可能是因为冗余技术使用，可减少或消除此问题。

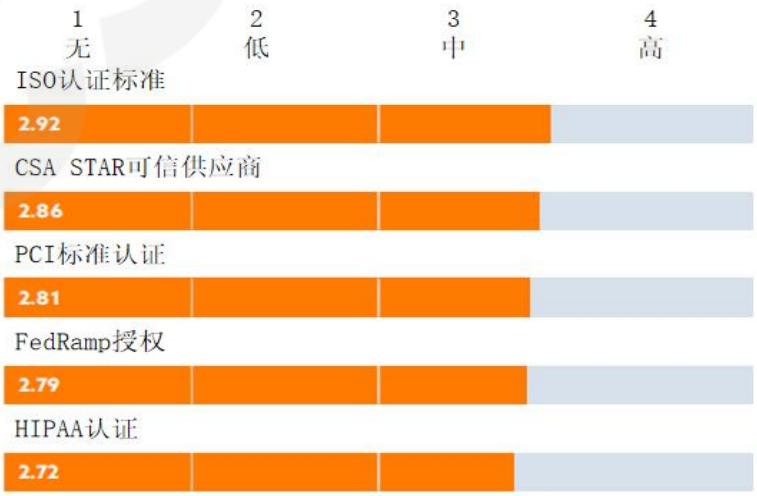
监管合规

监管合规的难度

无论环境如何，合规性都会给组织带来一定程度的挑战。本地部署的合规挑战仅仅略低于云服务或内部自研的应用程序。

第三方供应商进行安全合规认证的重要性

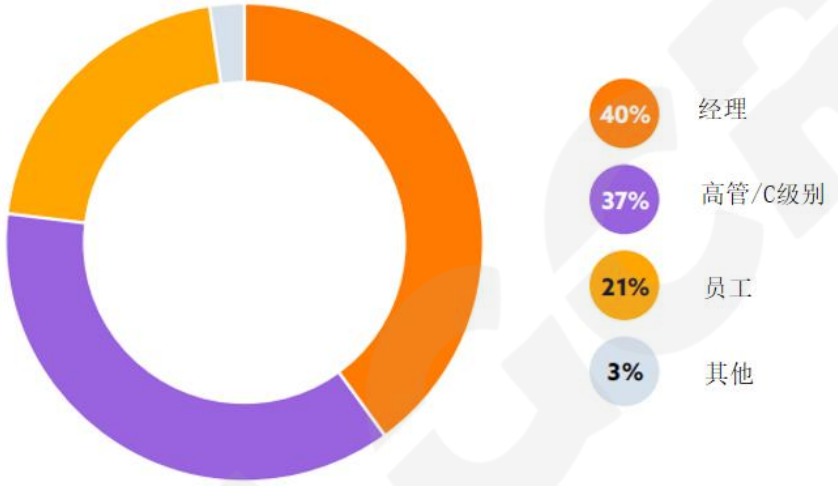
关于第三方供应商的安全合规认证，无论何种类型的认证，大多数认证对于组织重要性都处于中等重要水平。根据行业和组织使用的数据类型不同，重要性也会有不同。



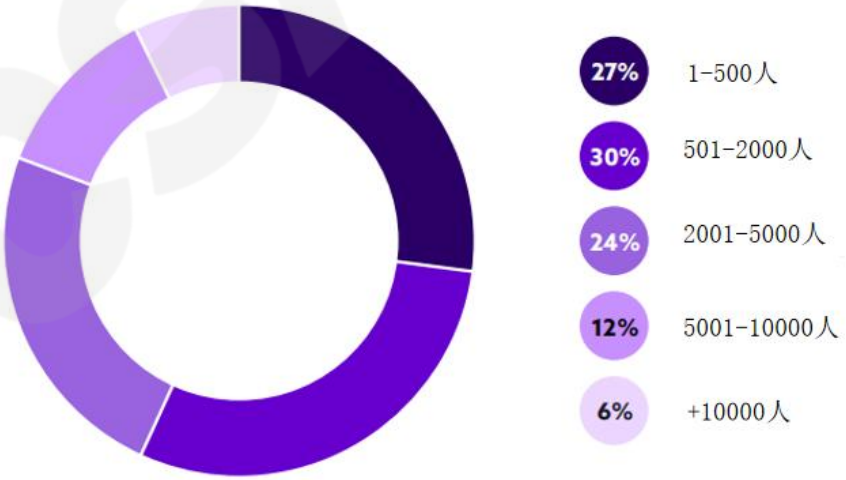
填定问卷的人员信息统计

这份调查在2022年7月进行，收集了1663份来自不同规模、行业、地区和角色的组织中IT和安全人员的调查问卷。

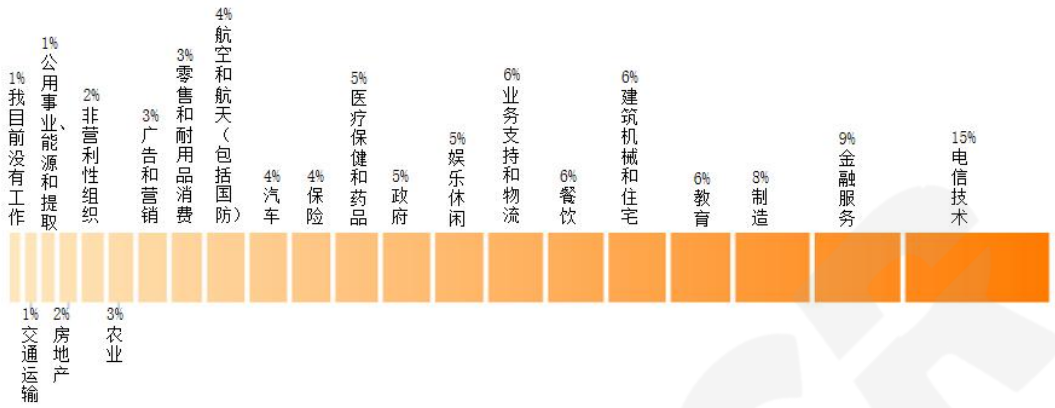
你的工作角色是什么?



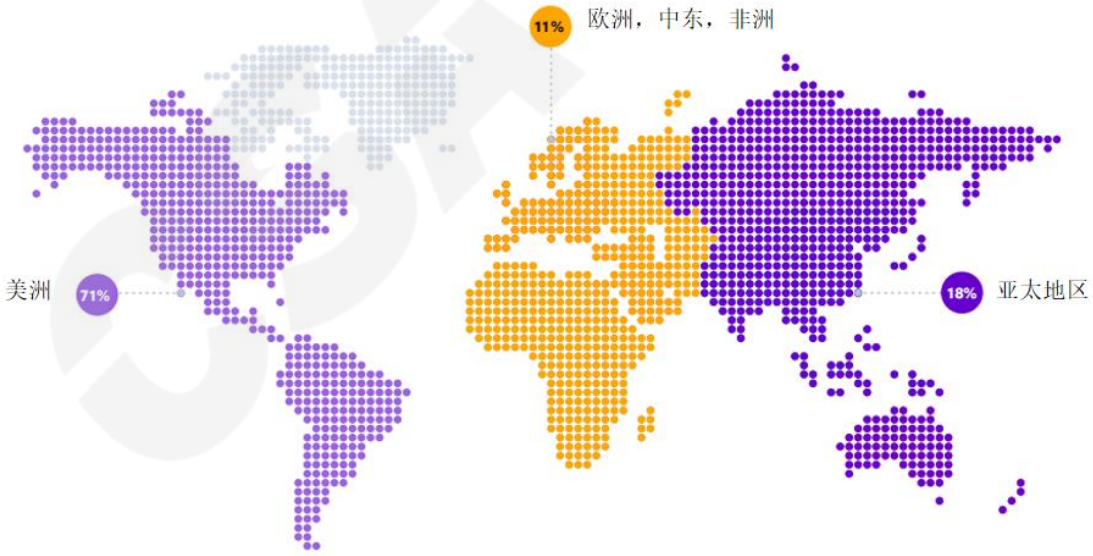
你所在的组织规模有多大?



以下哪一项最准确的描述了贵组织所在的主要行业?



您所在地区?



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