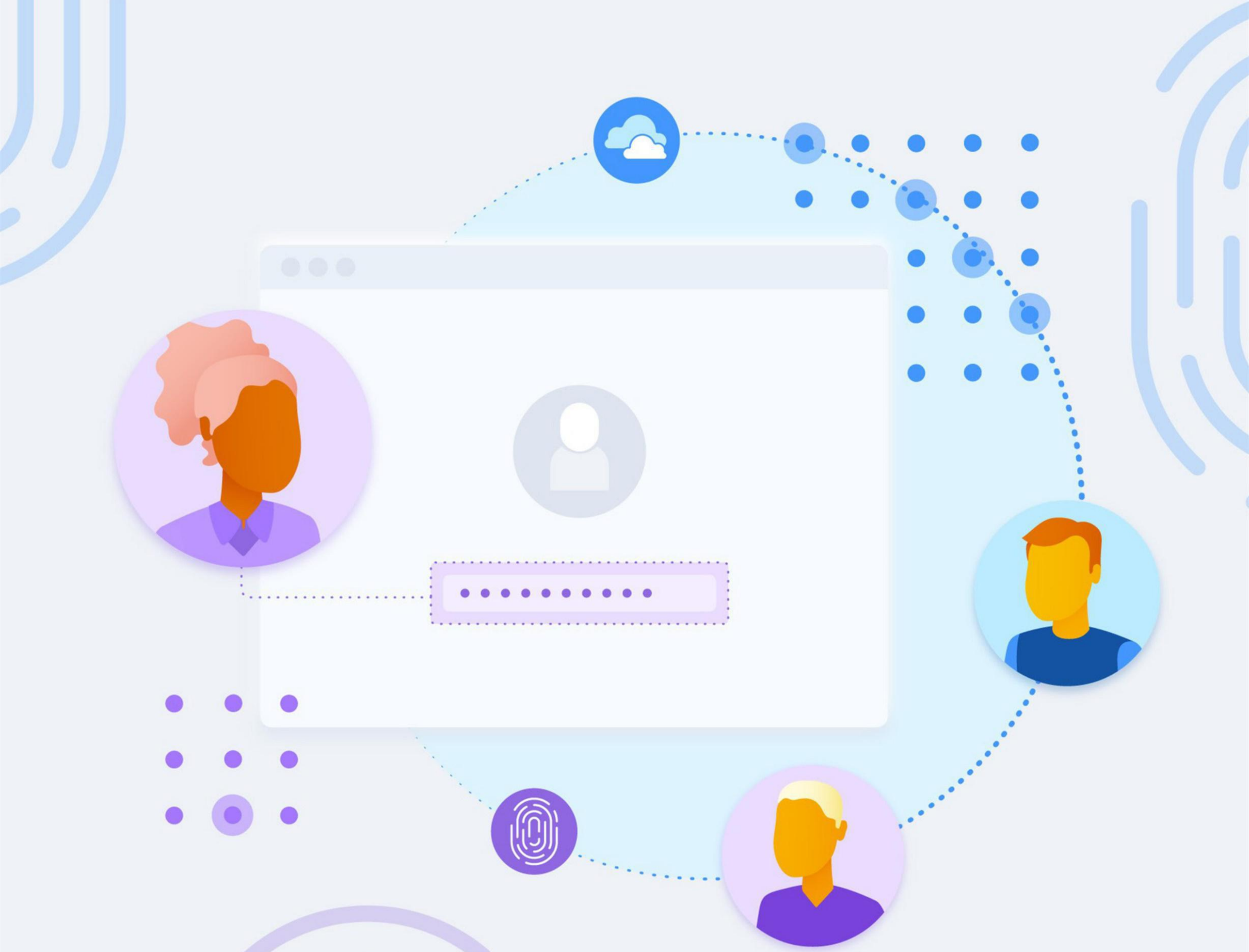
2020年云身份安全现状



CSA GCR GREATER CHINA REGION cloud security alliance®

CSA cloud security alliance®

中文翻译版说明

本文由云安全联盟大中华区（CSA GCR）IAM工作组专家对《The 2020 State of Identity Security in the Cloud》进行翻译审校。

翻译审校工作专家：

组长：戴立伟（竹云）

组员：程伟强（安讯奔）、郭晓锋（安讯奔）、史晓婧（竹云）、于继万（华为）、郭鹏程、江澎、薛琨、于乐、张帆（以上排名不分先后）

CSA大中华区研究助理：

朱晓璐

目 录

调研背景及方法

云安全联盟（CSA）作为非营利性组织，肩负着广泛推广云计算和IT技术中的网络安全最佳实践的使命。 CSA还承担着对云和IT技术从业者的教育和引导作用，使他们了解所有计算形式所面临的安全问题。CSA的成员众多，包括各行业从业人员、组织和专业协会。因此CSA的调研有助于评估各行业的信息安全技术成熟度和安全最佳实践落地情况。

在当前“新冠”疫情背景下，CyberArk委托CSA进行一项调研，以更好地了解未来12个月内云工作负载将面临的安全挑战，尤其是如何应对这些与身份和访问管理（IAM）相关的安全挑战。CyberArk与CSA共同制定了调研计划并编写了调查问卷，从2020年4月到5月，CSA共回收了近200份调查问卷。调研对象包括运营商及大型组织中经验丰富的云安全架构师、设计人员、运维人员等。CSA的专家小组对调研数据进行了分析，并根据分析结果起草了以下报告。

调研目标

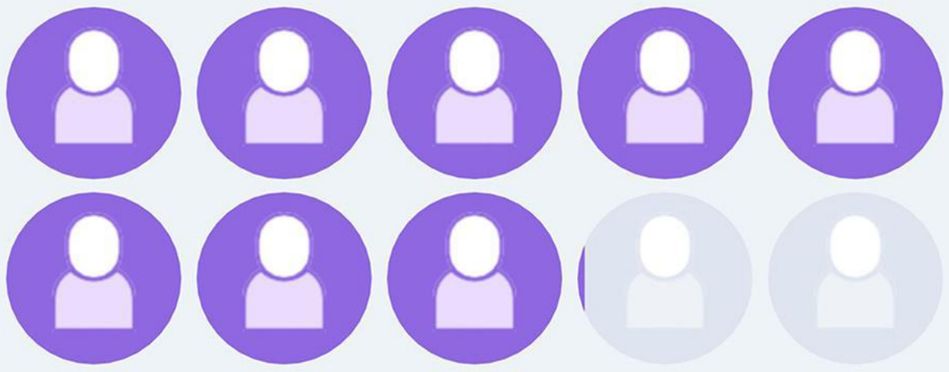
- 确定目前及未来一年公有云工作负载的使用和挑战
- 了解云IAM挑战，尤其是人和机器的身份识别挑战
- 制定应对云IAM挑战的预期方法
- 确定负责云IAM的团队和角色

摘 要

在过去的十年中，云服务的使用持续增长。 特别是在“新冠”疫情发生以后，许多企业的数字化转型加速进行，以使员工能够开展远程办公。 CSA对这些组织进行了调研，以更好地了解在此过渡期间组织如何使用云服务以及如何在未来12个月内保障其业务正常运营。

关键发现1

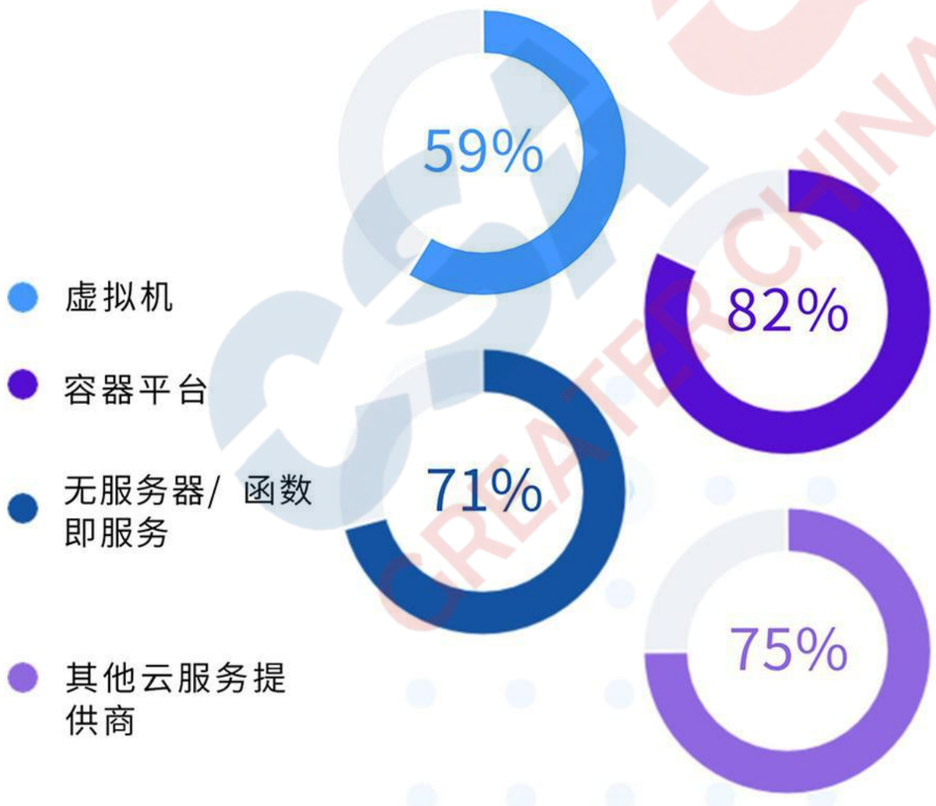
众多组织正在使用多云策略



81%的受访者表示其组织正在使用多云策略。但是，进一步的研究表明，他们严重依赖其中一家公有云提供商，而其他云提供商通常仅用于特定的工作负载。

顶级公有云提供商之间的市场份额逐渐趋于均衡，没有哪一家公有云厂商可以垄断整个行业。

公有云平台的使用使组织能够适应远程办公。 大多数企业正在使用多云策略，这增加了许多组织在安全性和可见性方面的挑战。 基于公有云平台进行开发的组织，越来越多地转向敏捷开发或基于DevOps的开发。



关键发现2

工作负载的类型有望增加

受访者期望工作负载的类型更加多样化。 除了传统的虚拟机用量将增加（占比59%），基于云的工作负载（例如容器平台）（占比82%）、无服务器/函数即服务（占比71%）和云服务（占比75%）的用量也会增加。

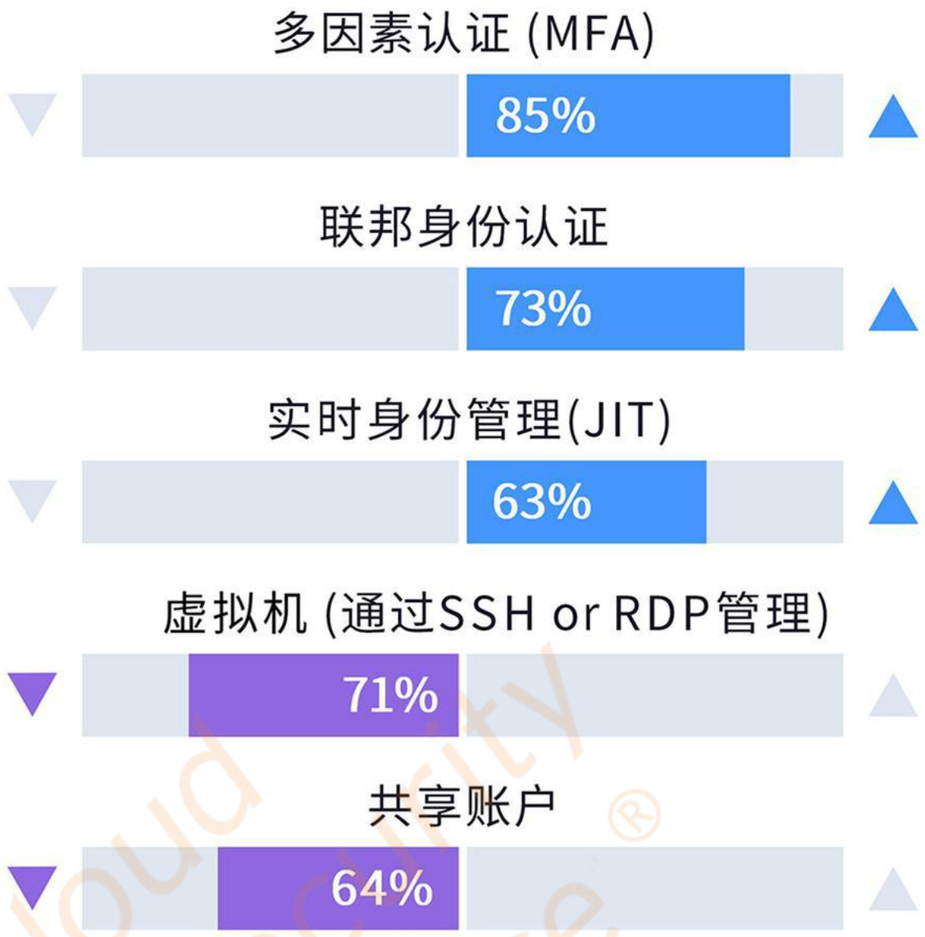
这些技术的使用可提高可移植性、敏捷性，并将安全能力嵌入代码中或实现安全前置(“左移”)。 DevOps生命周期中的安全前置确保在开发过程早期就内置安全，从而提升软件的质量。

越来越多的远程办公人员以及对云服务和基于云的开发技术的利用使办公环境变得更加复杂，因此需要额外的安全工具或策略来保障远程办公的身份安全。

关键发现3

组织对IAM功能的使用将发生变化

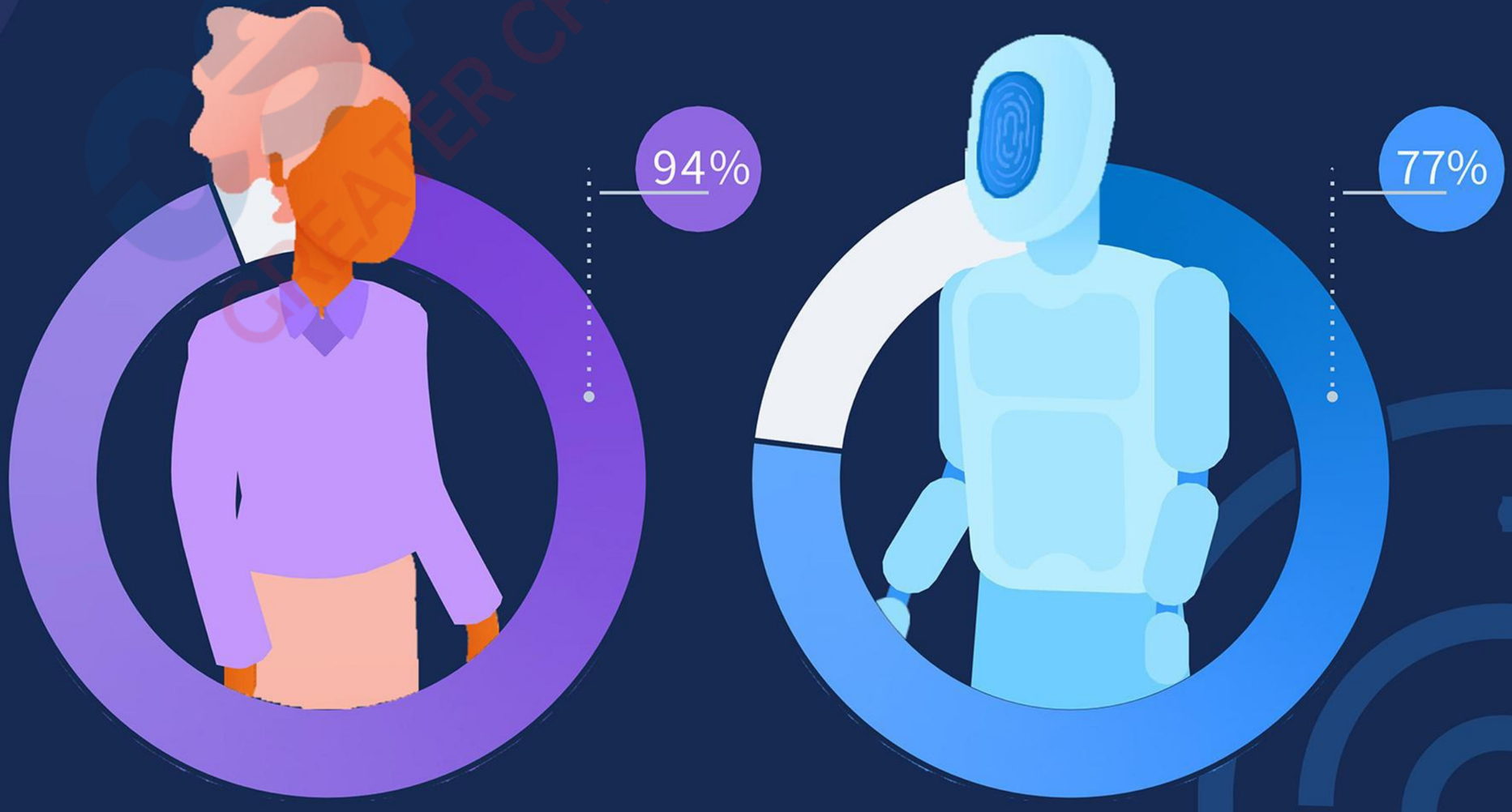
在本地或云上使用多因素认证（MFA）、联邦身份认证、实时身份管理Just in Time(JIT)、特权用户管理等IAM技术，能支持更细粒度的管控并降低安全风险。 许多接受调查的组织预测这些IAM技术的使用将增加，同时将利用云服务提供商的IAM功能，此外还将整合第三方身份服务供应商的能力来满足这些需求。



关键发现4

不管是针对人还是机器，特权和权限管理均被认为是IAM安全的首要挑战。

特权和权限管理被认为是人员身份（94%）和机器身份（77%）的头等大事



众多组织正在使用多云策略

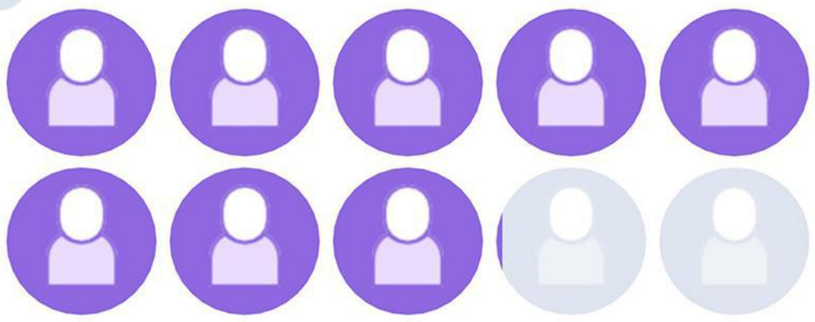
顶级公有云提供商之间的市场份额逐渐趋于均衡，没有哪一家公有云厂商可以垄断整个行业。

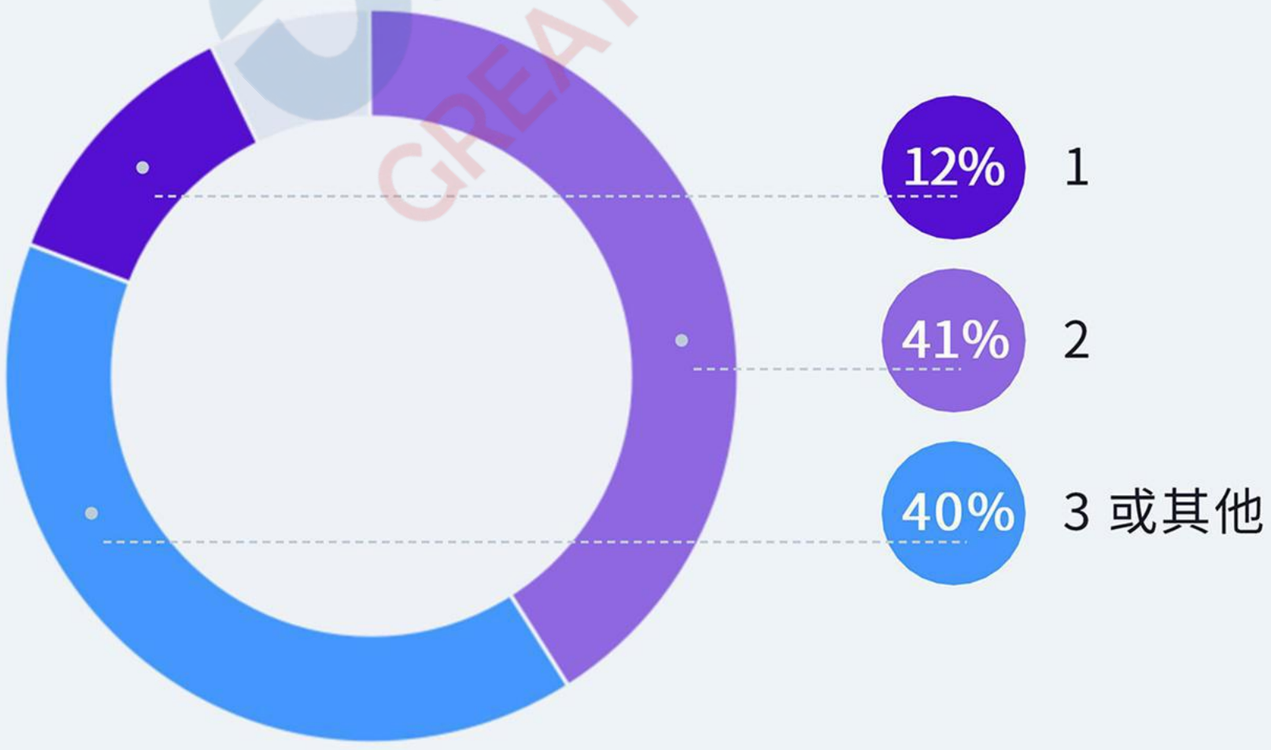
组织使用的主要的公有云平台

*Azure包括Azure、Azure AD 和 O365

大多数组织将需要使用多云策略

然而，许多组织严重依赖单一公有云提供商。其他提供商通常仅用于特定的工作负载。





组织使用的公有云平台数量

随着公有云工作负载类型的增加，组织面临的安全挑战也会增多

工作负载使用变化预测

受访者预测未来一年中，容器平台、函数即服务/无服务器和云服务的使用都将增加。虚拟机的使用也会增加。

工作负载面临的5大安全挑战预测

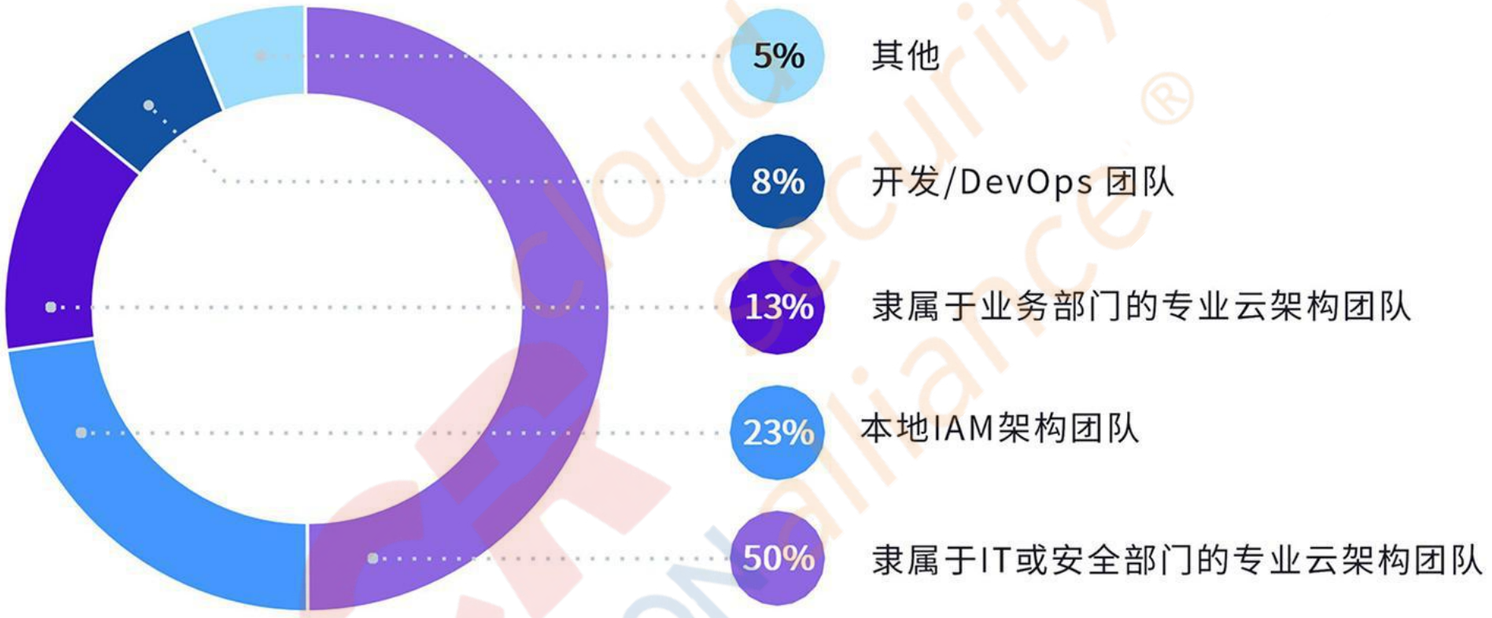
受访者预测未来一年云工作负载面临的前5项安全挑战是可见性、数据隐私、IAM流程、配置管理和合规性。

1 可见性
2 数据隐私
3 IAM流程
4 配置管理
5 合规性

负责云IAM架构、设计和运维的团队因组织而异

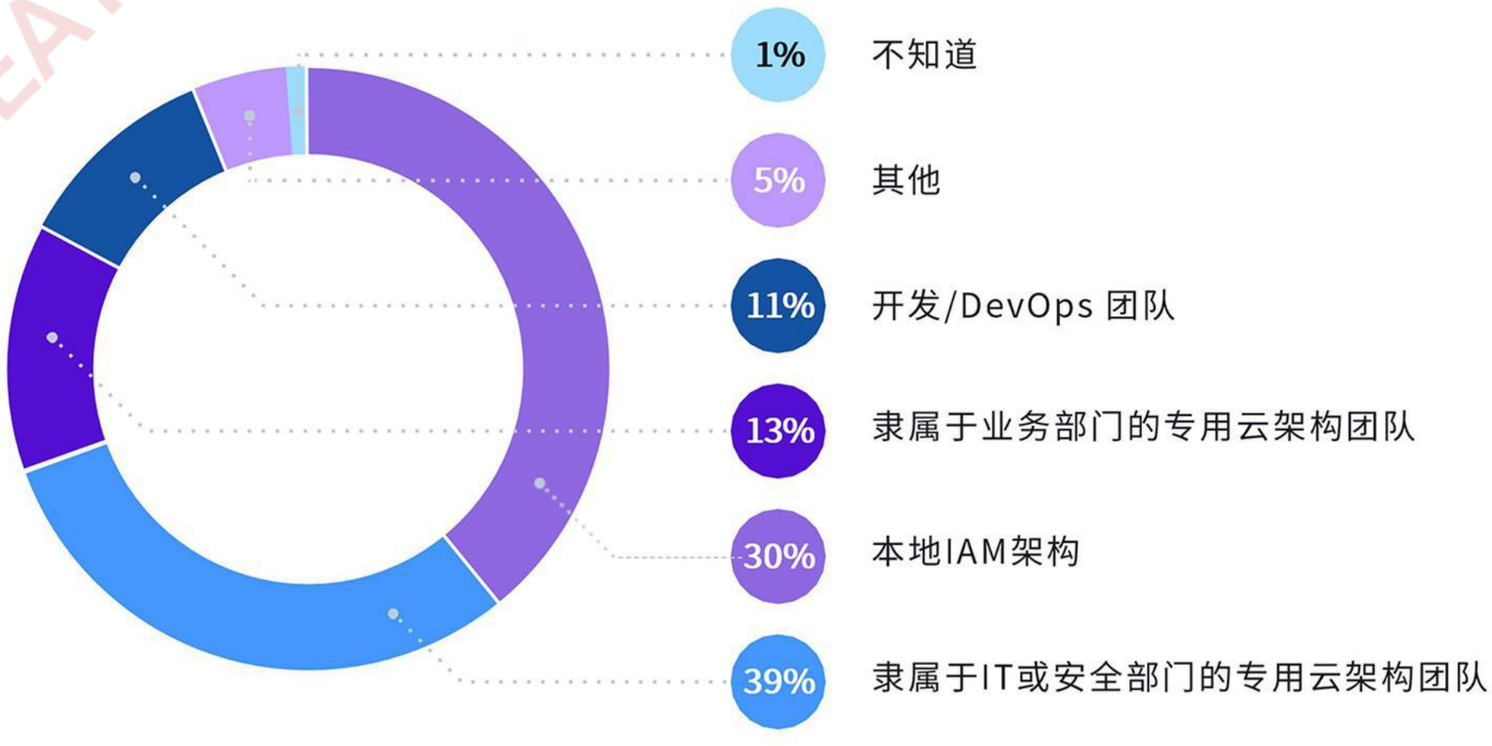
不同的组织负责云IAM架构和设计的团队也不一样。最常见的是由隶属IT或安全部门的专业云架构团队负责(占比50%)，其次是由本地IAM架构团队负责(占比23%)，也有的组织是由业务部门的专业云架构团队负责(占比13%)，只有8%的人表示是由开发/DevOps团队负责。

负责云IAM架构和设计的团队



负责云IAM运维的团队也不尽相同。最常见的是由隶属于IT或安全部门的专用云架构团队负责(占比39%)，其次是由本地IAM架构团队负责(30%)，也有的组织是由隶属于业务部门的专业云架构团队负责(13%)，只有11%的组织是由开发/DevOps团队负责。

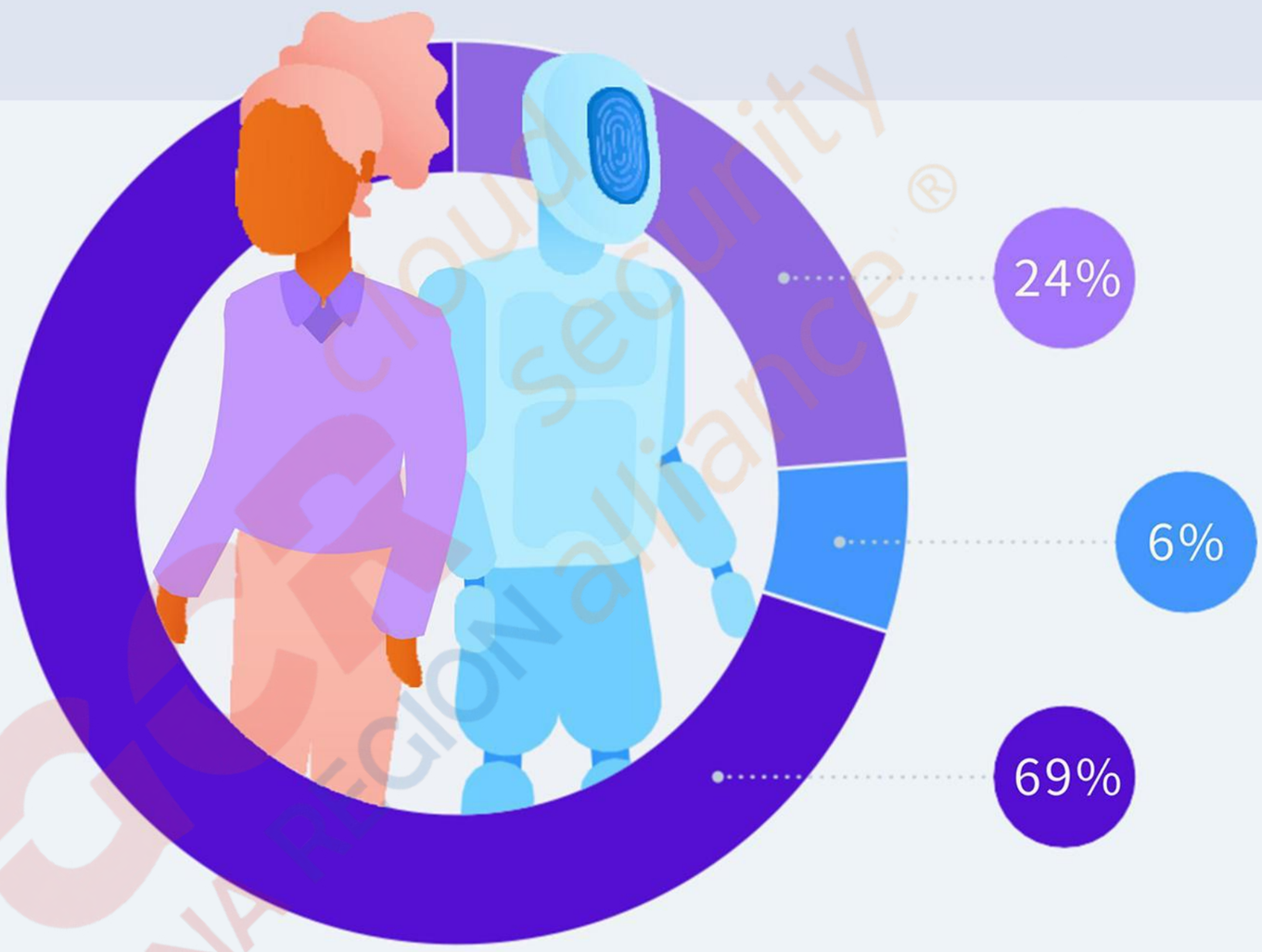
负责云IAM运维的团队



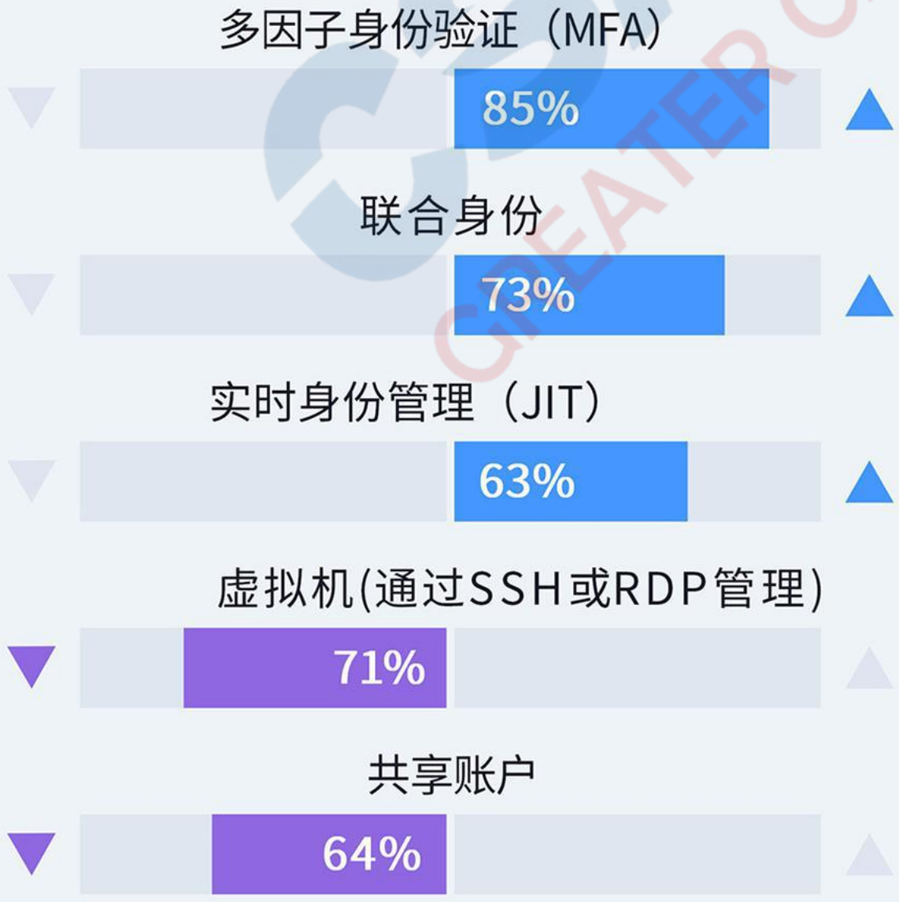
组织对 IAM 功能的使用将发生变化

69%的受访者认为人员访问安全和机器访问安全同等重要，约24%的受访者认为人员访问安全比机器访问安全更重要，只有 6%的组织认为机器访问安全更重要。

机器访问安全与人员访问安全哪个优先级更高



- 人员访问安全优先
- 机器访问安全优先
- 人员和机器同等优先级



预计未来一年，组织对公有云IAM功能的使用将发生变化

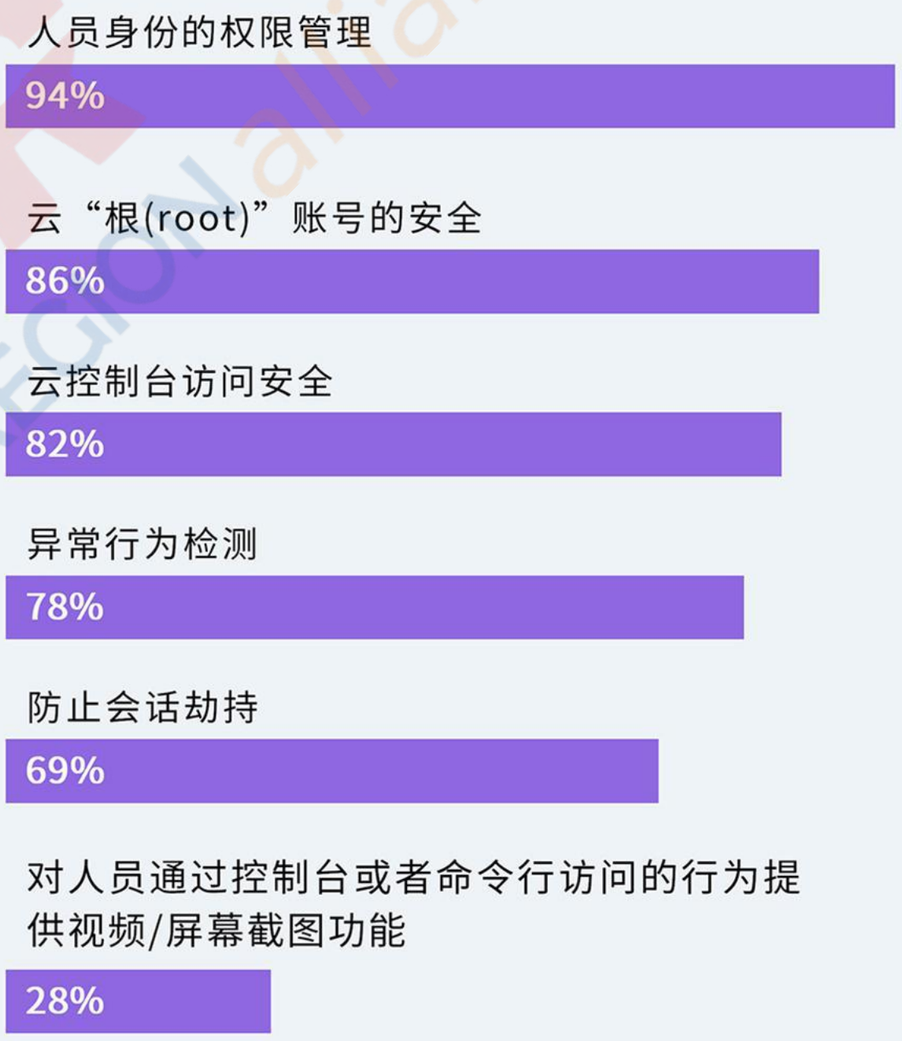
组织计划在明年将IAM功能向公有云迁移。高级MFA、联邦身份认证和 实时身份管理JIT 的使用率预计分别增加85% 、73% 和63% 。然而，通过SSH和RDP对虚拟机的交互式访问和共享帐户的使用预计将分别减少71%和64%。

特权和权限管理被认为是IAM的首要安全挑战

人员身份安全面临的挑战：

- 人员身份的权限管理
- 云“根(root)”账号的安全
- 云控制台访问安全
- 异常行为检测
- 防止会话劫持
- 对人员通过控制台或者命令行访问的行为提供视频/屏幕截图功能

人员身份安全挑战的优先级排序

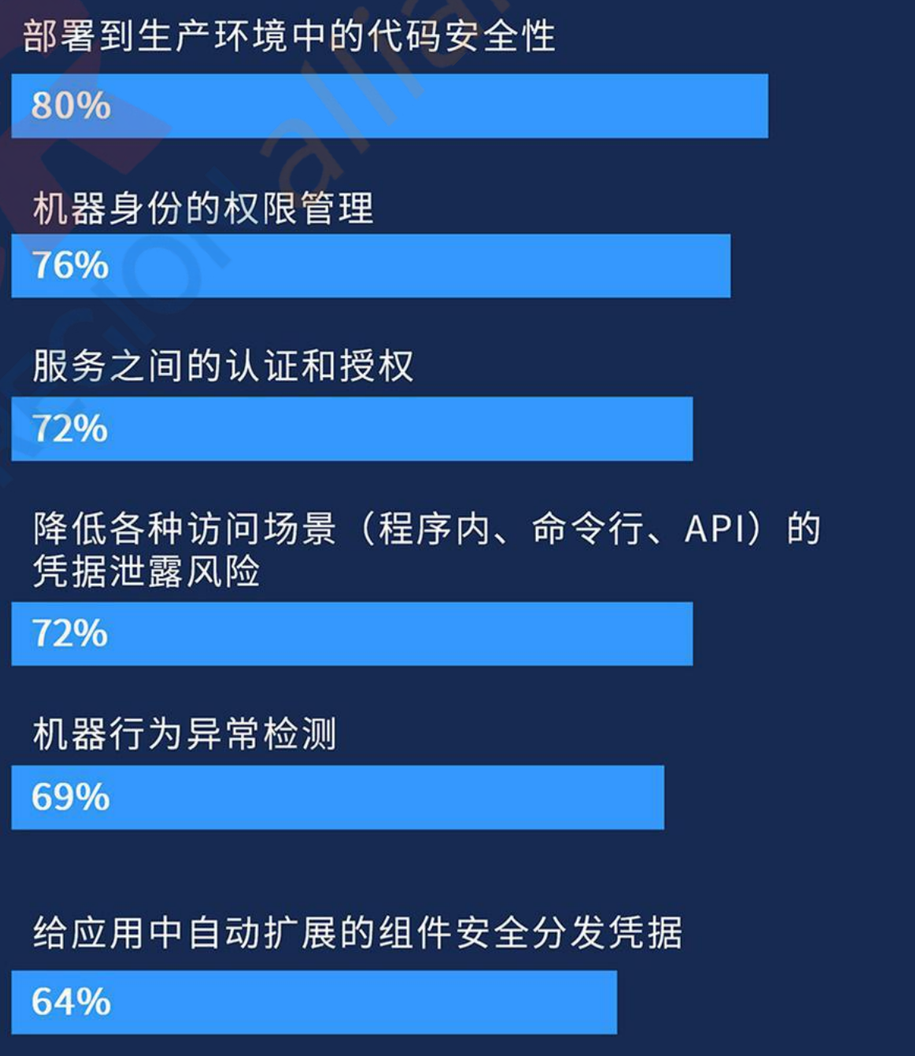


受访者还被问及该组织在机器身份管理方面所面临的安全挑战的优先级。以下所有内容都被认为是高优先级事项：安全部署到生产环境、机器权限管理，服务之间的认证和授权，降低各种访问场景（程序内、命令行、API）的凭据泄露风险，机器行为异常检测，给应用中自动扩展的组件安全分发凭据。值得注意的是，不管是机器身份还是人的身份，权限管理都被认为是最高优先级。

机器身份安全面临的挑战：

- 部署到生产环境中的代码安全性
- 机器身份的权限管理
- 服务之间的认证和授权
- 降低各种访问场景（程序内、命令行、API）的凭据泄露风险
- 机器行为异常检测
- 给应用中自动扩展的组件安全分发凭据

机器身份安全挑战的优先级排序

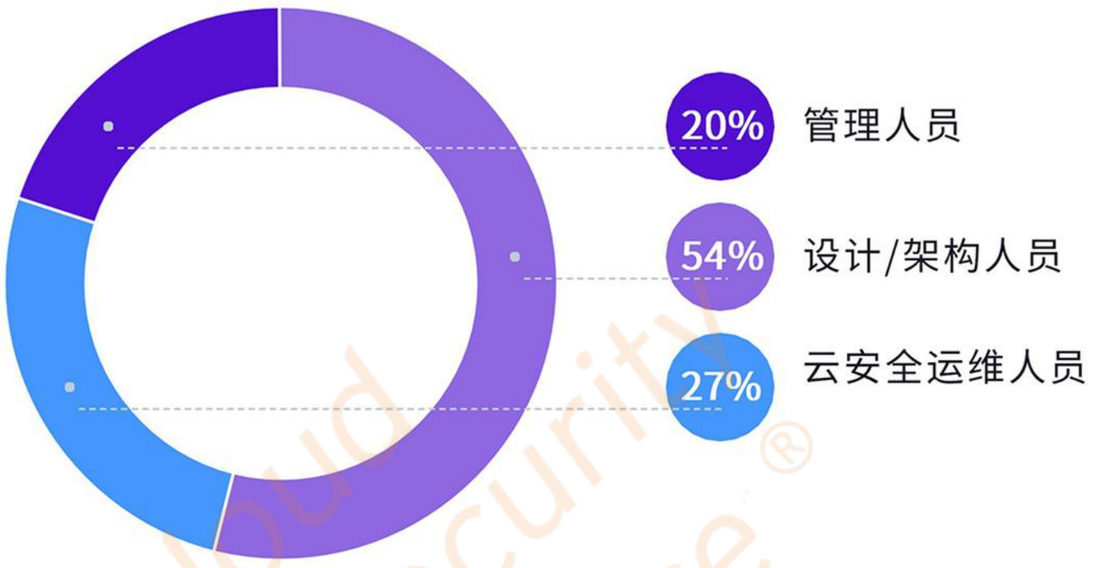


受访者还被问及该组织在机器身份管理面临挑战的优先级。以下所有内容都被认为是高优先级事项：安全部署到生产环境、机器权限管理，服务之间的认证和授权，降低各种访问场景（程序内、命令行、API）的凭据泄露风险，机器行为异常检测，给应用中自动扩展的组件安全分发凭据。值得注意的是，不管是机器身份还是人的身份，权限管理都被认为是最高优先级。

受访者的背景

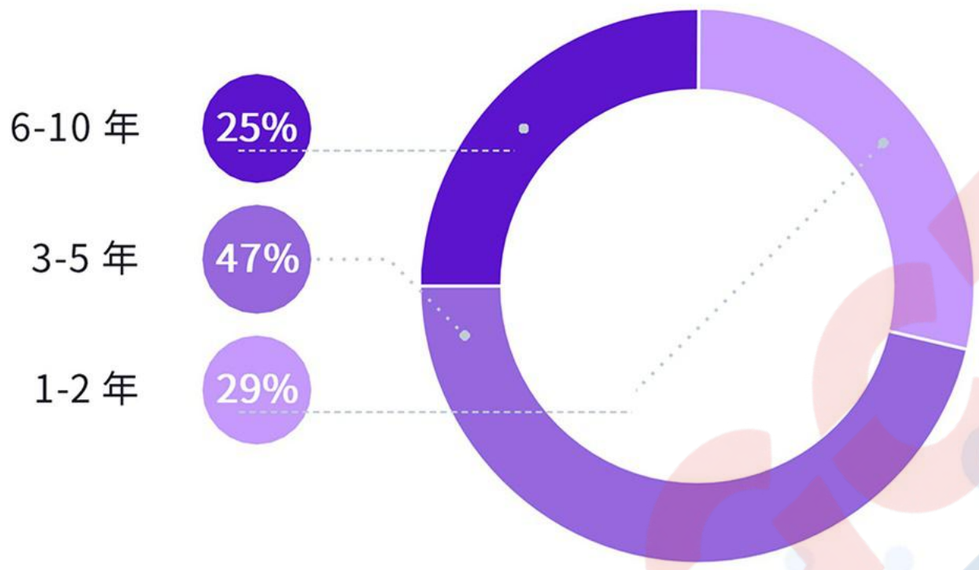
工作角色

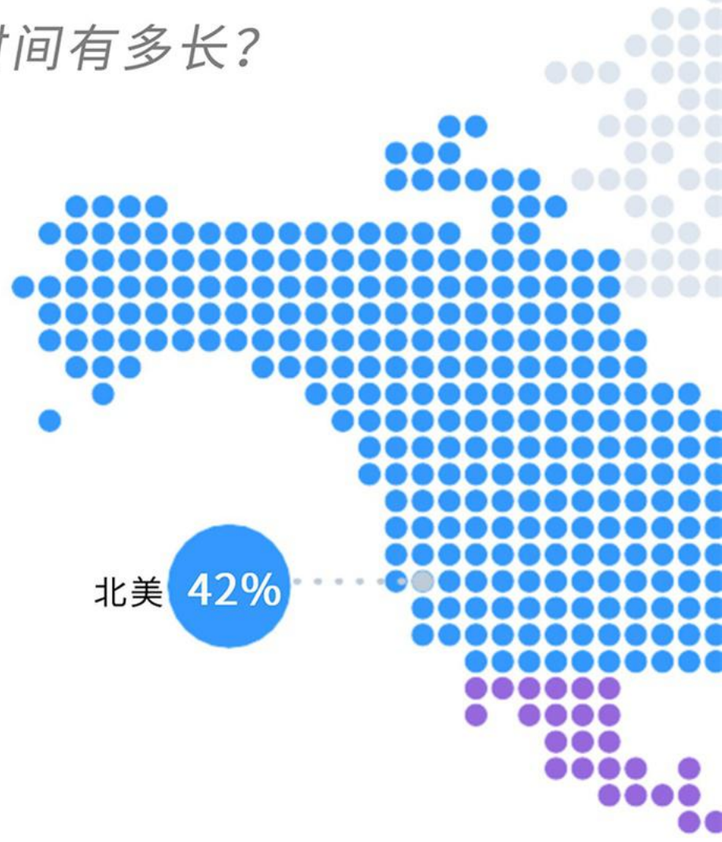
以下哪一项最能正确描述您在云安全工作中承担的主要职责?



工作年限

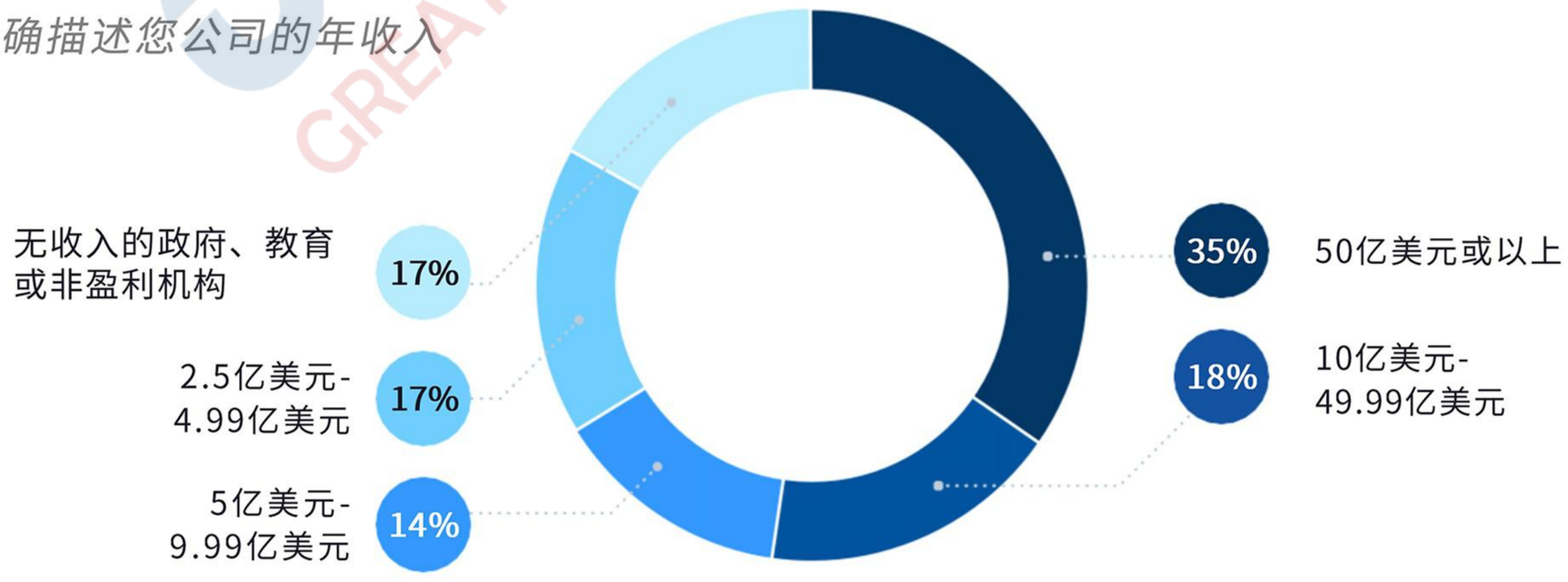
您从事云安全的时间有多长?





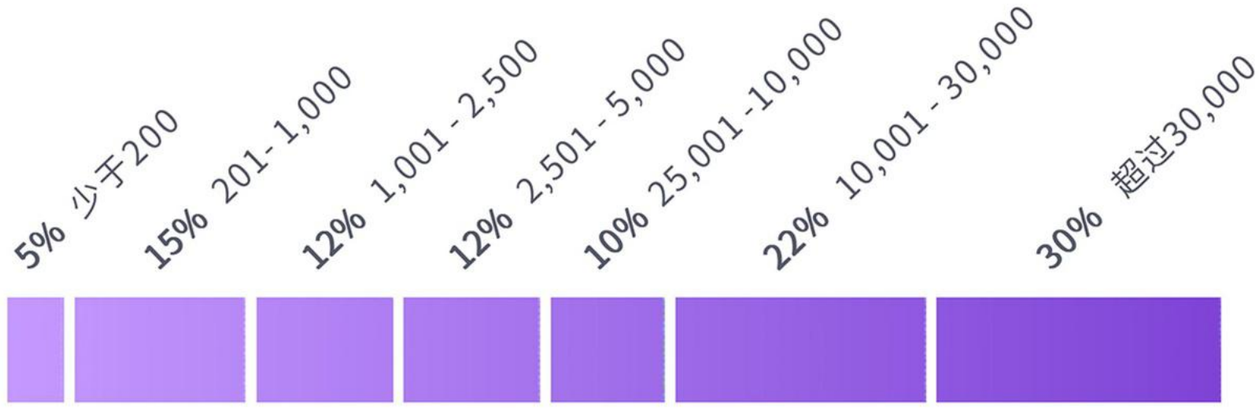
公司营收

据您所知，以下哪个范围最能正确描述您公司的年收入



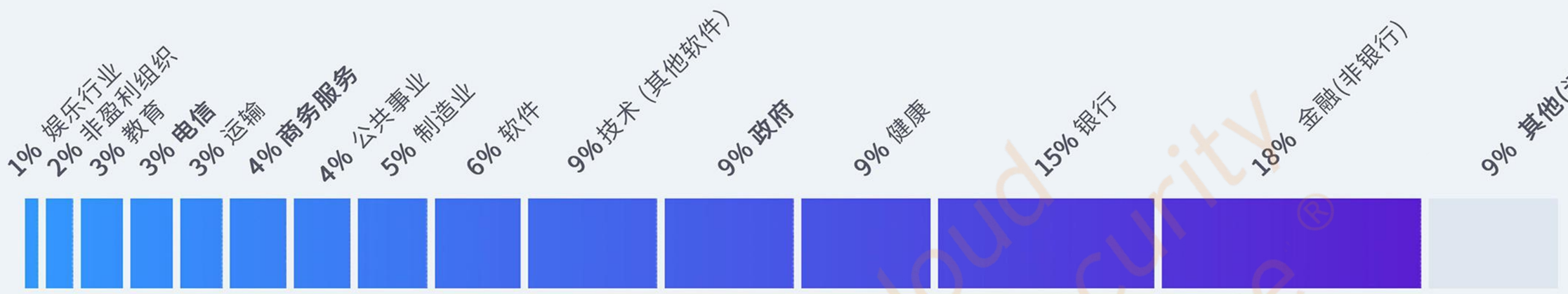
公司规模

以下最能描述公司/组织中员工人数的是?



所属行业

贵公司属于什么行业?



位置（按国家）

您主要位于哪里?