CISO研究报告

零信任的部署现状及未来展望

CSA GCR cloud security alliance GREATER CHINA REGION

CSA cloud security alliance®

CxO信托工作组官网网址：

https://cloudsecurityalliance.org/research/working-groups/cxo-trust-working-group/

致谢

《CISO 研究报告：零信任的部署现状及未来展望（CISO Perspectives and Progress in Deploying Zero Trust）》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：陈本峰

翻译组：何国锋　苏泰泉　汪 海

审校组：姚　凯

研究协调员：潘国强　李　杰

感谢以下单位的支持与贡献：

启明星辰信息技术集团股份有限公司　　云深互联(北京)科技有限公司

中国电信研究院安全技术研究所

英文版本编写专家

主要作者：Hillary Baron　　John Yeoh

贡献者：Illena Armstrong　　Josh Buker　　Daniele Catteddu

Sean Heide　　Alex Kaluza　　Claire Lehnert (design)

Stephen Lumpe (design)　　Jim Reavis

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

当今，数字化浪潮汹涌奔腾，各行各业都在加速推进企业数字化转型进程，云计算、大数据、移动互联网、物联网、5G 等技术广泛应用，远程办公、业务协同、分支互联等业务需求快速发展。与前所未有的网络互联应用规模相对应的，是精准投放的高级网络攻击频发，给组织带来巨大损失，而传统安全防护理念在层出不穷的新型网络威胁面前显得力不从心。

零信任概念于2010年首次提出,，假定入侵已经发生（而不是假定公司防火墙背后的所有内容均是安全的），并将每个请求视为源自开放网络。无论请求源自何处，无论请求访问何种资源，都应坚守“永不信任，始终验证”原则。这种理念的提出，为网络安全解决方案的设计提供了全新思路，认为可有效应对新型网络威胁和先进攻击手段。业界普遍认为零信任方案可与更多数字应用场景和安全功能结合，应用规模将持续扩大。

2021年5月，美国总统拜登发布了14028号行政令《改善国家网络安全》，要求联邦政府机构应制定零信任架构实施计划。随后，美国联邦政府多个部门提出了一系列关于零信任的战略规划和指南，将对零信任的关注度推上了新的高度。

但是零信任作为一种新兴的解决方案，在推广和应用过程中不可避免地会遇到一些问题，零信任的先行实践者们在面对这些问题时也存在一些困惑，这些问题和困惑的存在阻碍了零信任方案的广泛推广。

作为零信任的重要推动者，CSA一直专注于零信任方案的研究与创新。 CSA在2014年发布了《软件定义边界SDP标准规范1.0》，2022年发布了《软件定义边界SDP标准规范2.0》，并发布了《实战零信任架构》、《SASE安全访问边缘白皮书》等一系列规范和报告，为零信任业界提供了重要的参考。

为了帮助业界分析零信任研究和实践过程中遇到的问题，CSA组织了本次调研，通过广泛的意见收集和统计，尝试揭示零信任方案落地过程中的障碍。期望通过这些分析，帮助业界找到解决问题的方案。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

执行摘要

零信任理念已经存在了十多年。然而最近，对需要保护IT系统的企业来说，这个术语及其实施方式的关注度存在显著增加。随着数字化转型的推进、疫情期间的工作方式转变，以及美国网络安全行政命令的发布，零信任已经被认为是企业安全的首选方案。

标准开发组织（SDOs）最近启动了关于零信任的工作（例如NIST SP 800-207）。同样，其他相关机构和组织也开始发布指南、建议和基础文献。由于标准化现状相对不成熟、词汇表和行业定义不统一、以及标榜零信任的供应商解决方案的多样性，让人们产生了困惑。这促使CSA展开了对零信任的理解、认知和应用情况的行业调研。

本次CSA调研的目的是为了更好地理解组织机构内部的零信任策略。安全从业者们要求评估以下方面:

- 零信任在组织机构中的成熟度和优先级
- 应用零信任的好处和驱动因素
- 应用零信任的挑战和障碍
- 支持零信任战略所需的投资

调研涉及的其他一些领域包括：零信任在组织机构中的什么位置处于优先地位、完成相关实施的组织机构比例、最顶端的业务挑战和技术挑战。

本次分享的初步研究成果，是由包括219名CxO高管在内的，来自不同地区且组织规模各异的823名IT和安全专业人员反馈的情况。调研结果揭示一些有趣的发现，包括:

- 80%的C级高管（副总裁以上）将零信任作为组织的优先事项
- 94%的人正在实施零信任战略
- 77%的人在未来12月里会增加零信任支出

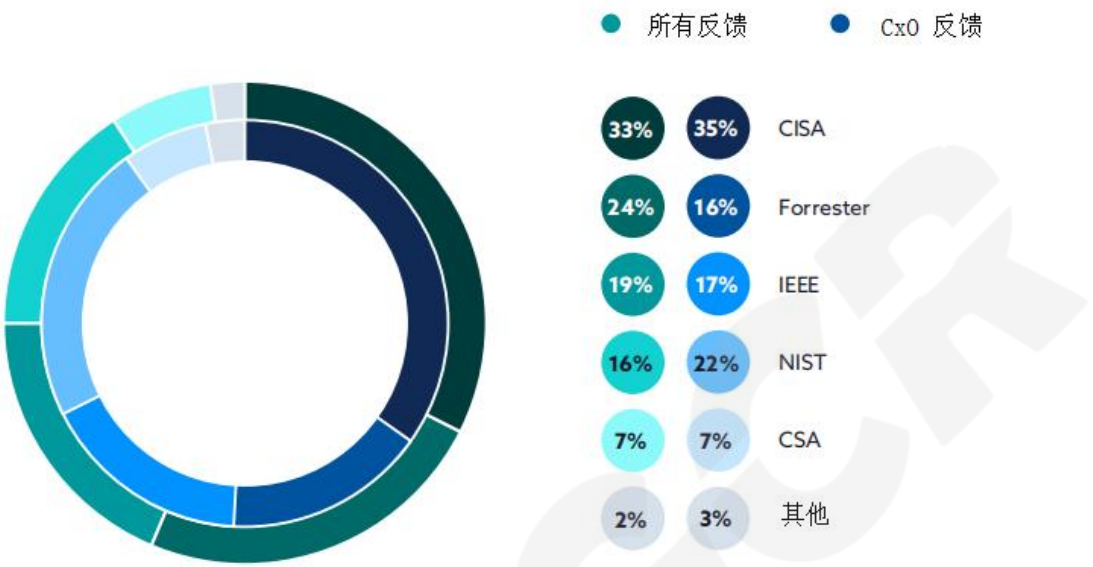
对调研结果的进一步分析将使CSA能够协助针对访问控制、策略实施、零信任扩展问题和由受访从业者处发现的其他挑战，定义一系列指南。通过本次调研及即将发布的报告，CSA希望了解CxO高管零信任战略、痛点、供应商需求、管理要求/监督、技术考虑、历史遗留问题、应用率，以及利益相关方的参与情况。CSA致力于让CxO高管、董事会成员、员工

和利益相关方了解零信任的好处。

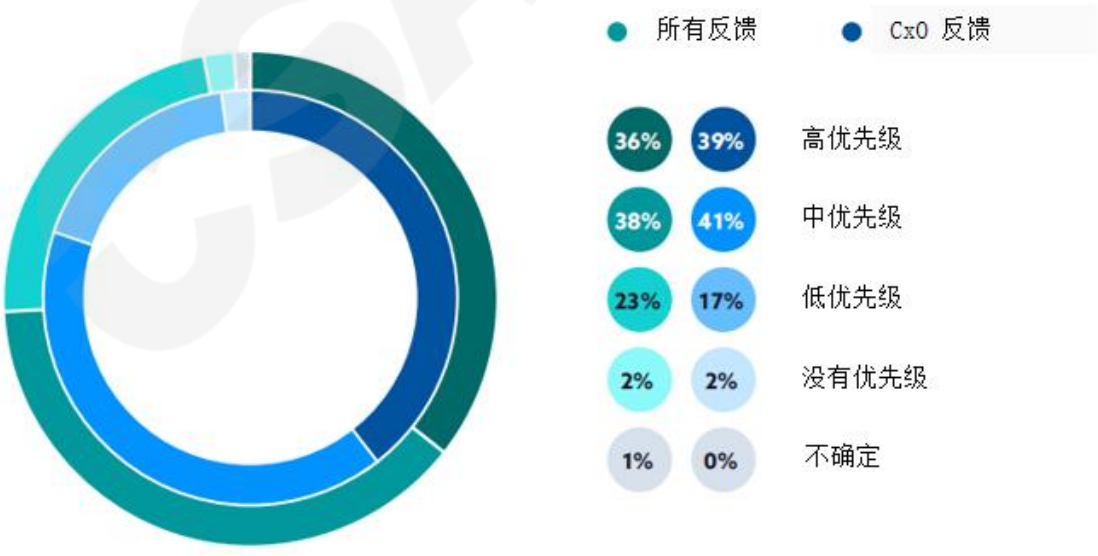
调研报告将基于2022年第1到第3季度CSA从调查反馈及访谈中收集到的认知与意见。CSA社区的零信任研究人员、分析师和行业专家将根据收集到的数据提供进一步的观察结果和统计相关性。

国际云安全联盟（CSA）是一个非营利性组织，其使命是广泛推广最佳实践，保障云计算和IT技术的网络安全。CSA还向这些行业中的各种利益相关方提供关于其他计算形式的安全问题教育。CSA的会员是一个由行业从业者、企业和专业协会组成的广泛联盟。CSA的主要目的之一是开展调查以评估信息安全趋势。这些调查提供了组织当前关于信息安全和技术方面的成熟度、意见、兴趣和意向等信息。

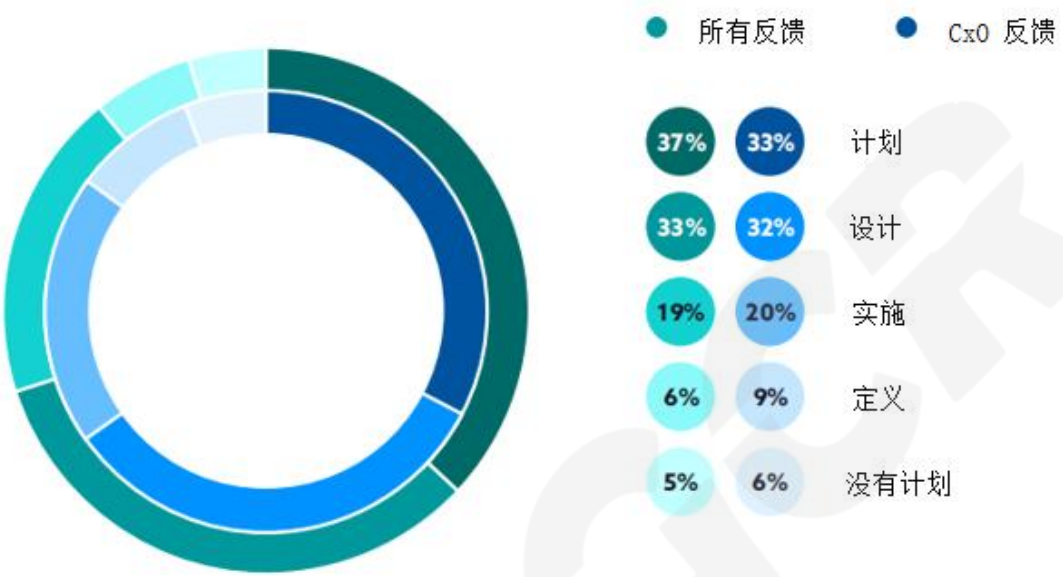
以下哪项行业指南最符合您的组织机构对零信任的定义/指导方针?



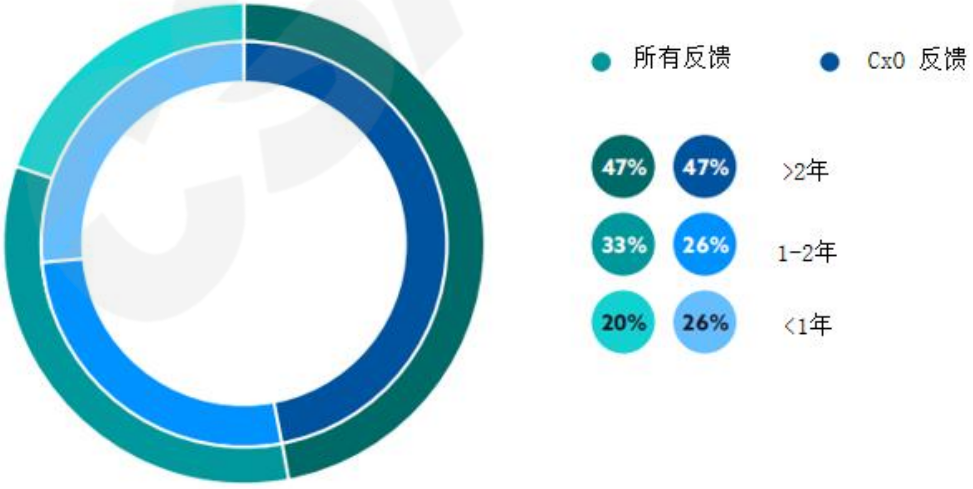
零信任在您的组织机构中处于什么优先级?



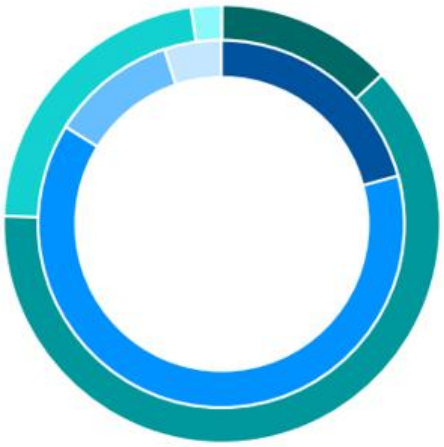
在零信任战略的实施过程中，你的组织机构处在什么阶段？



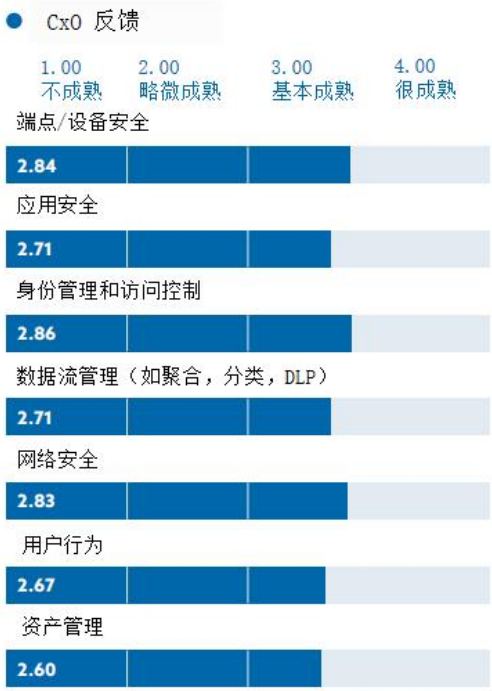
您的组织机构最初是什么时候实施零信任战略的？



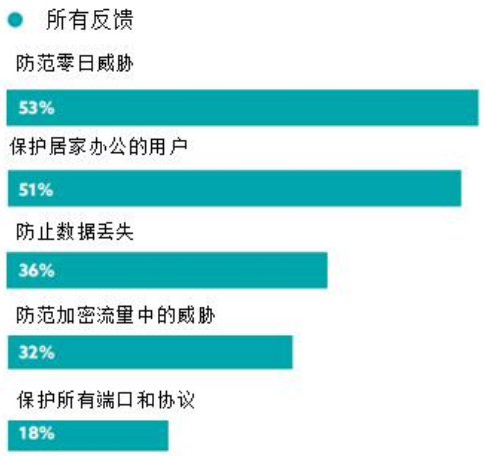
您的组织机构是否从零信任计划中受益？

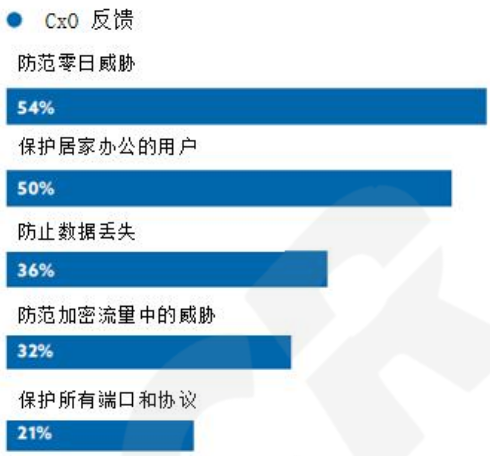


请在以下方面评估组织机构的零信任战略的成熟度：

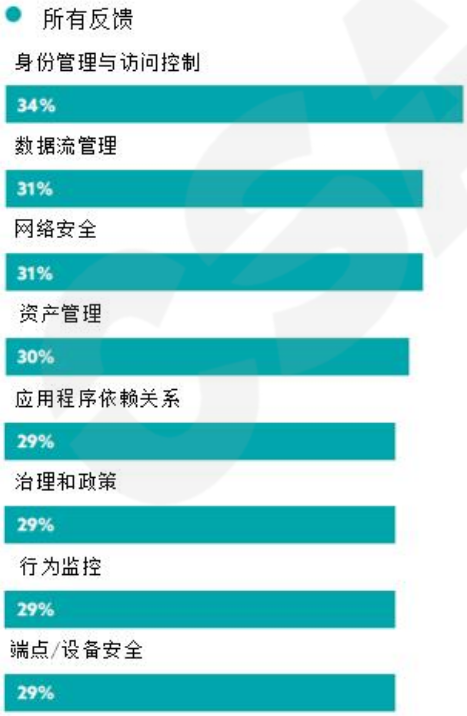


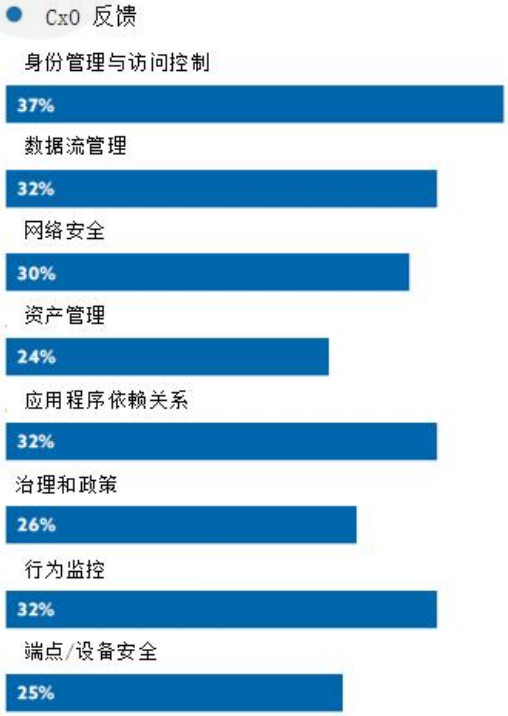
您公司在哪个方面感到最脆弱？





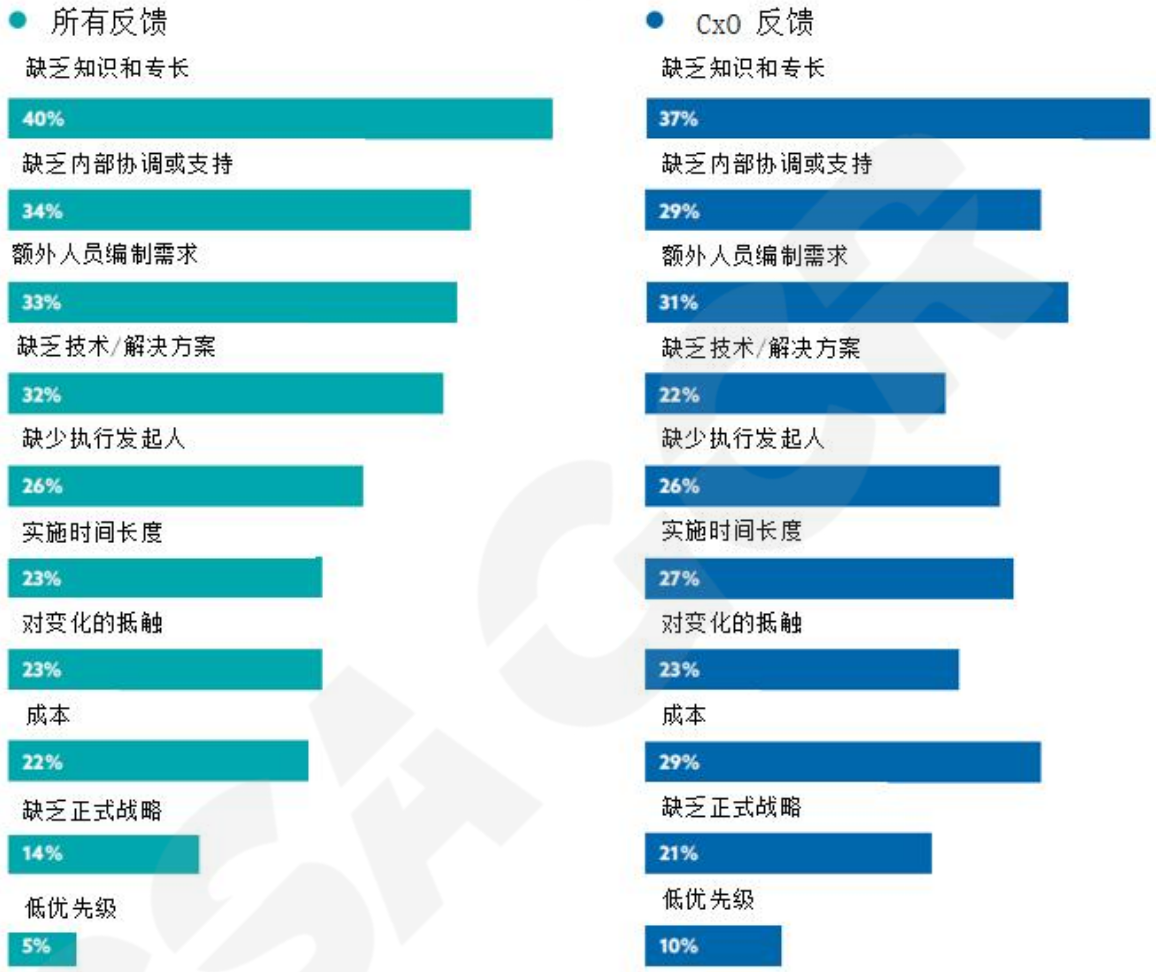
选出您的组织机构采用零信任的3大困难



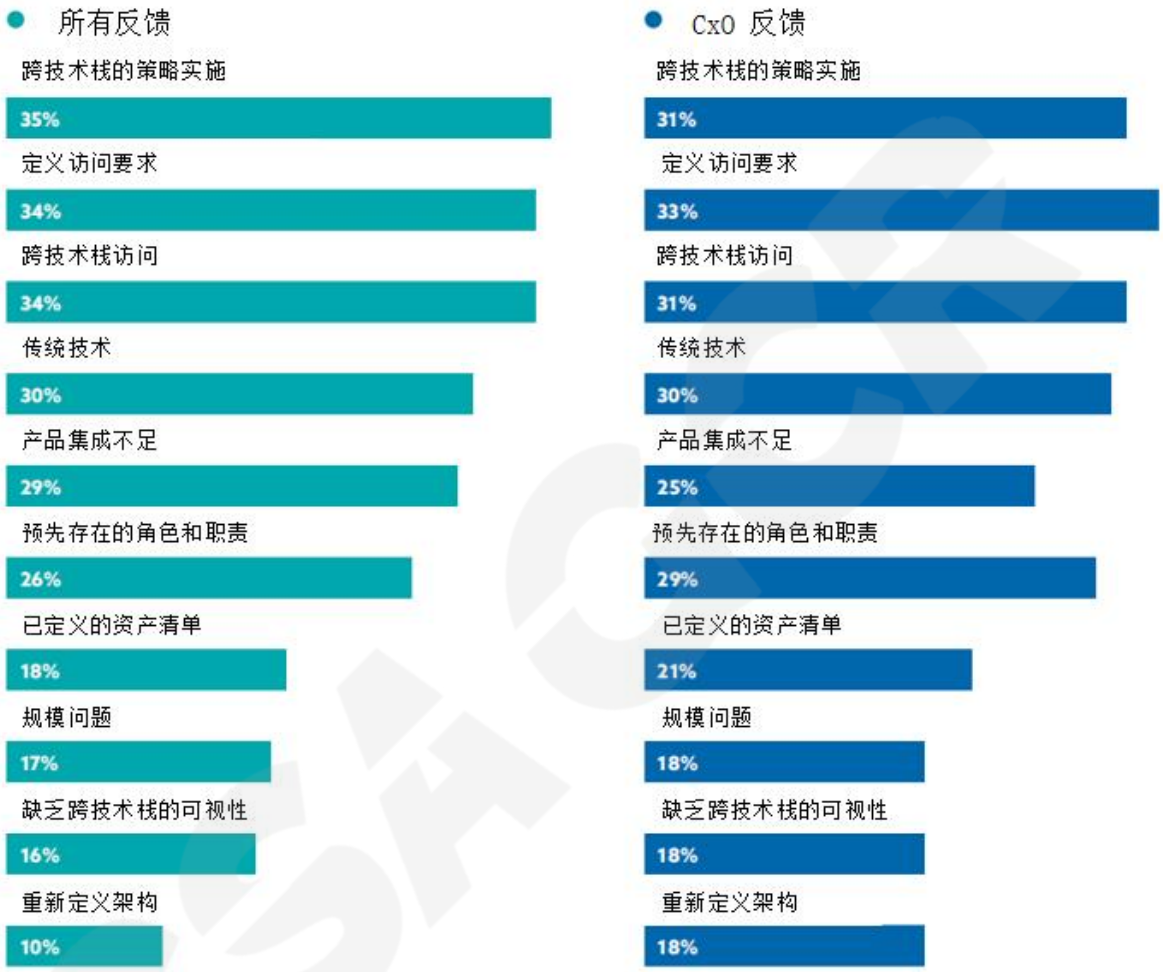


您的组织机构采用零信任计划的主要驱动因素是什么？（最多选择3个）

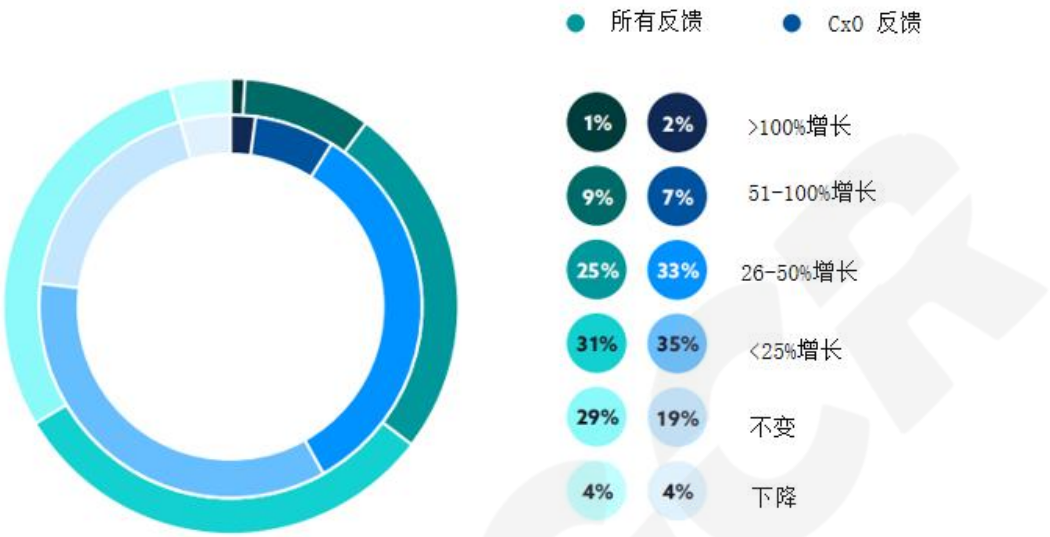
您的组织机构采用零信任战略的最大业务障碍是什么？（最多选3项）



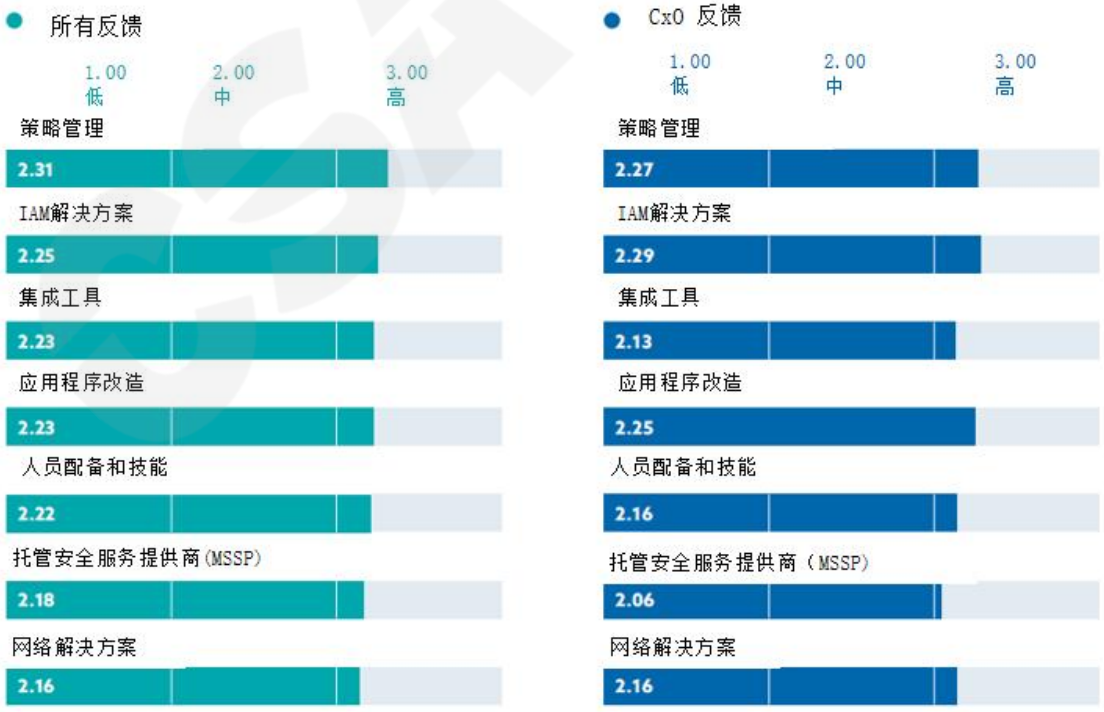
您的组织机构采用零信任战略的最大技术障碍是什么？（最多选3项）



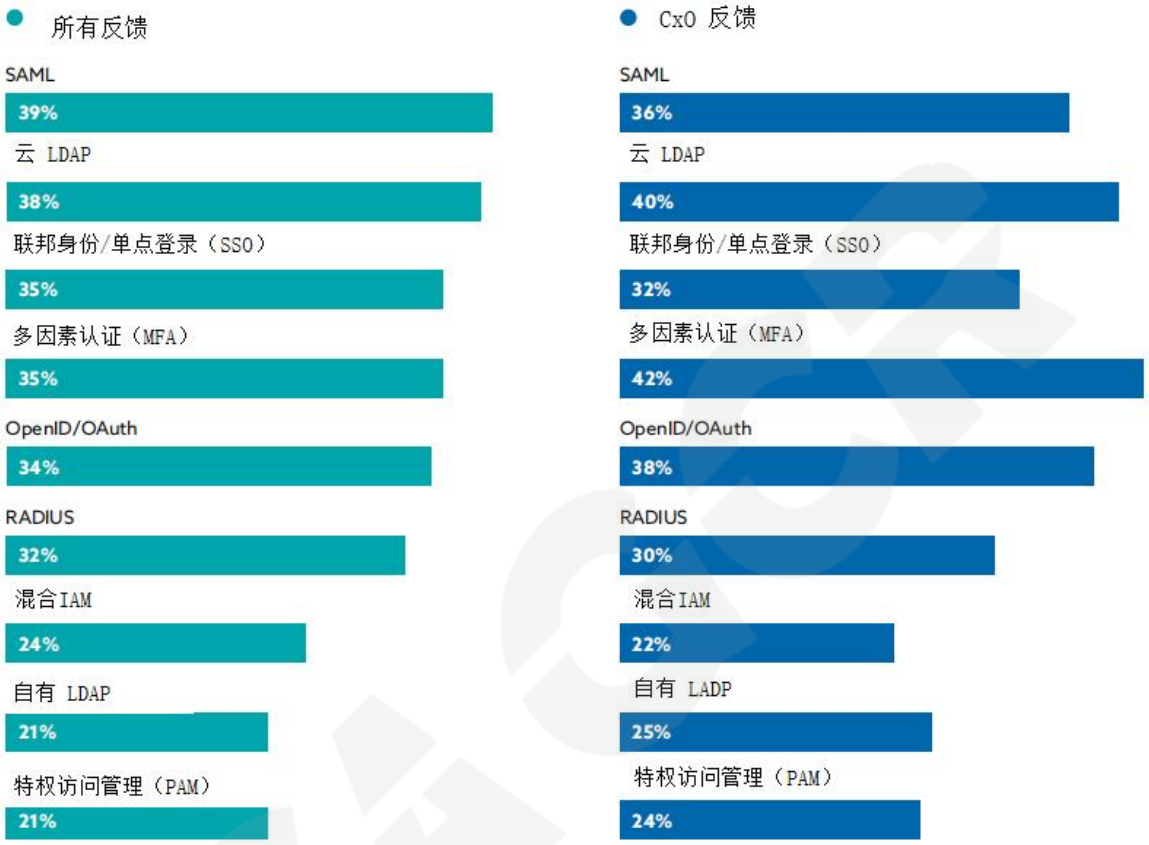
请描述您的组织机构未来12个月内在零信任计划上的投资情况



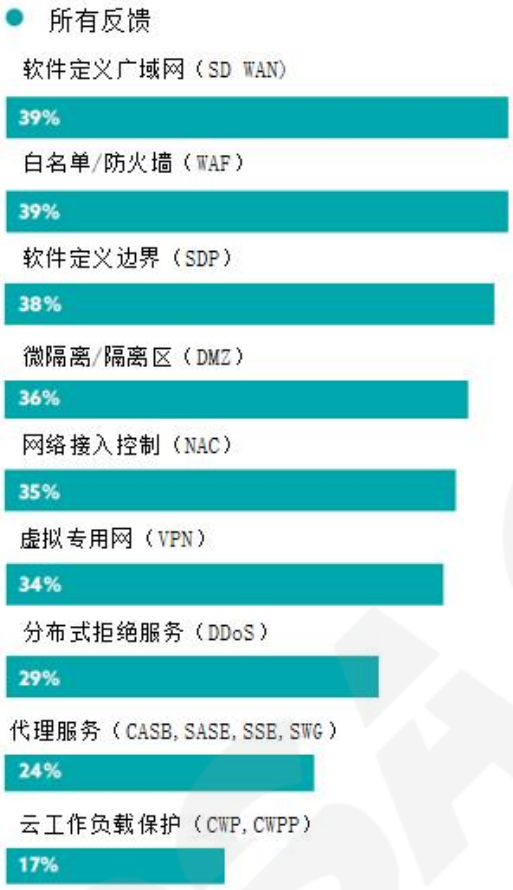
对于零信任计划，您的组织机构在以下类型的解决方案上各投入了多少资金？

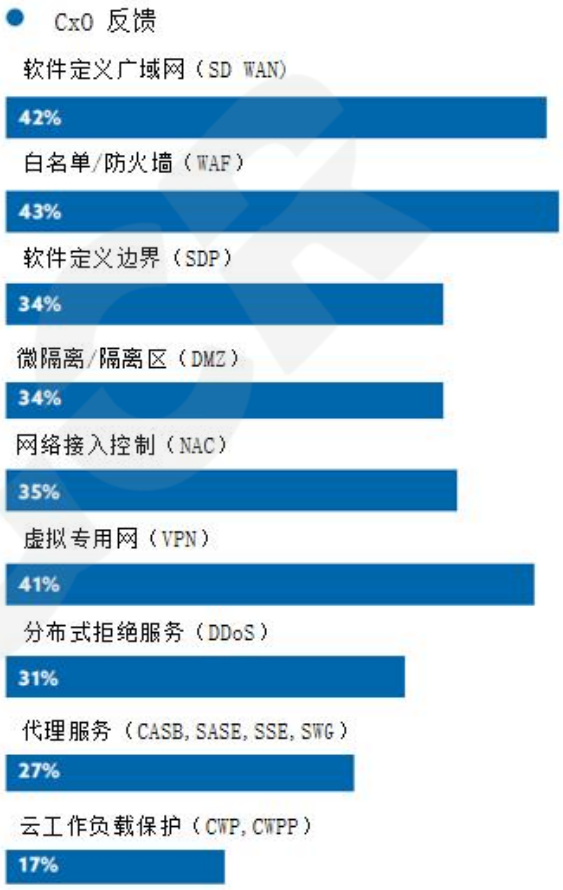


您的组织机构采用了哪些类型的身份服务？（多选）

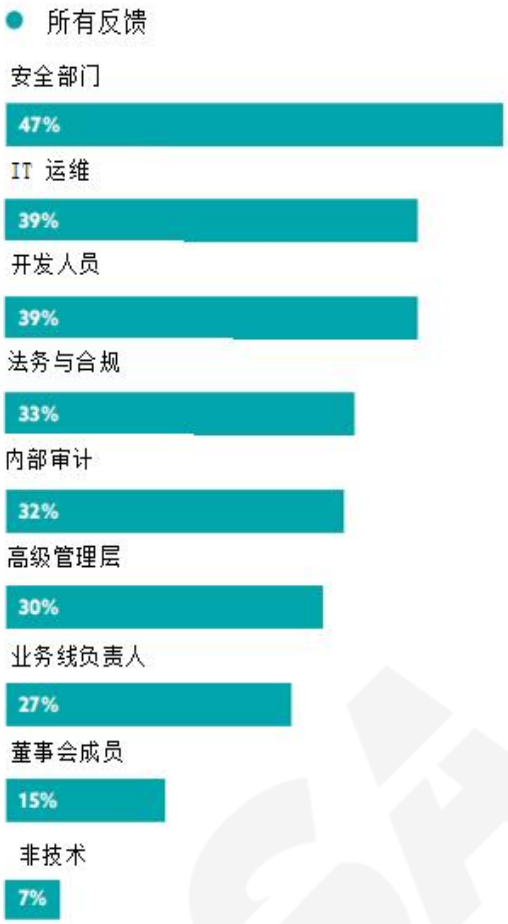


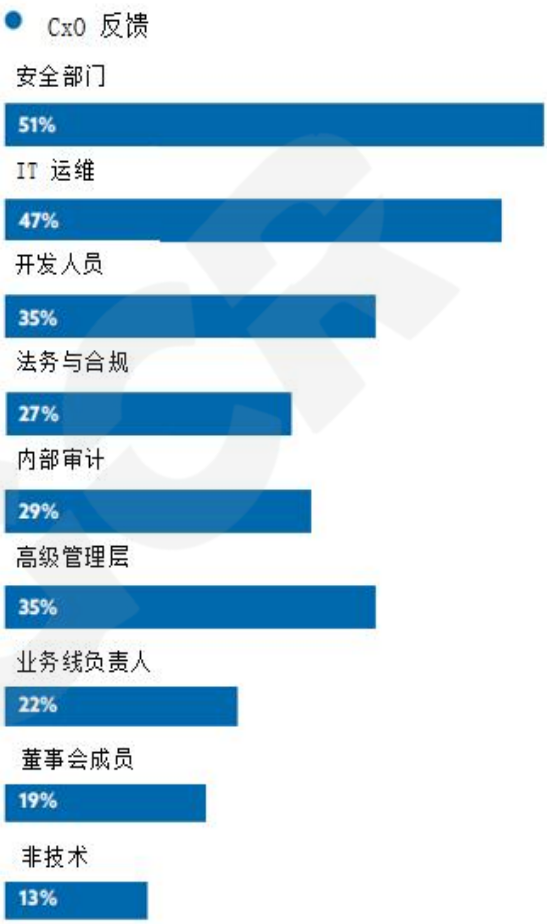
您的组织机构采用了哪些类型的网络解决方案？（多选）



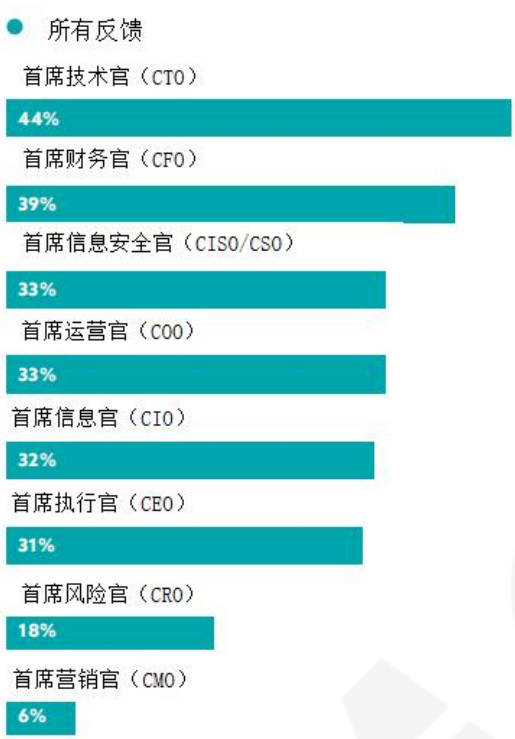


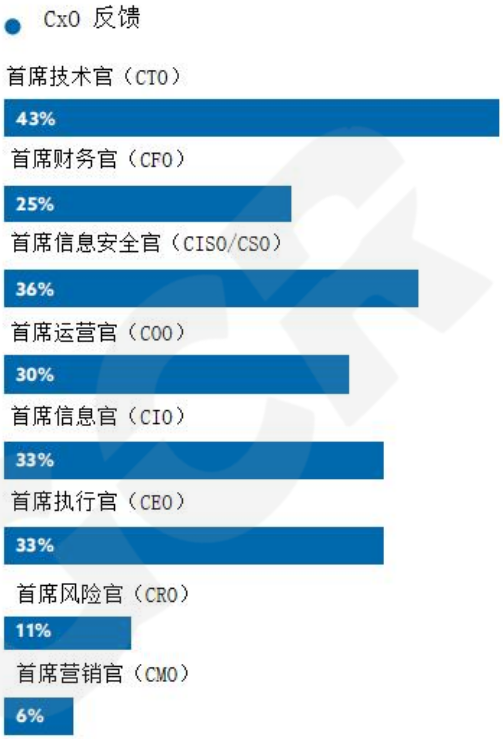
您的组织机构中实施零信任会涉及哪些业务部门？（多选）





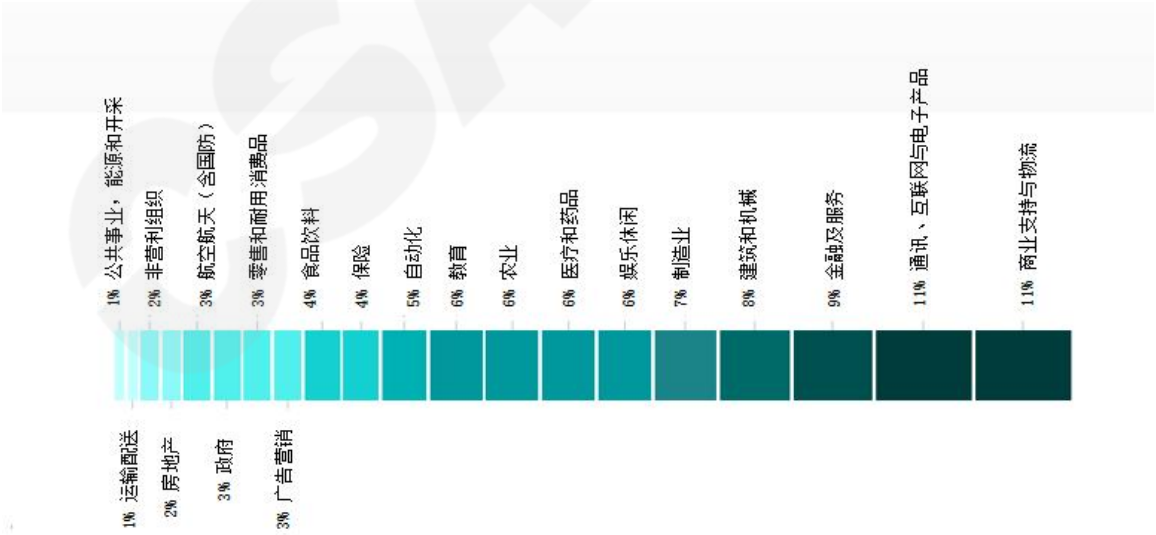
您的组织机构中哪些高管负责或支持零信任的实施部署？（多选）



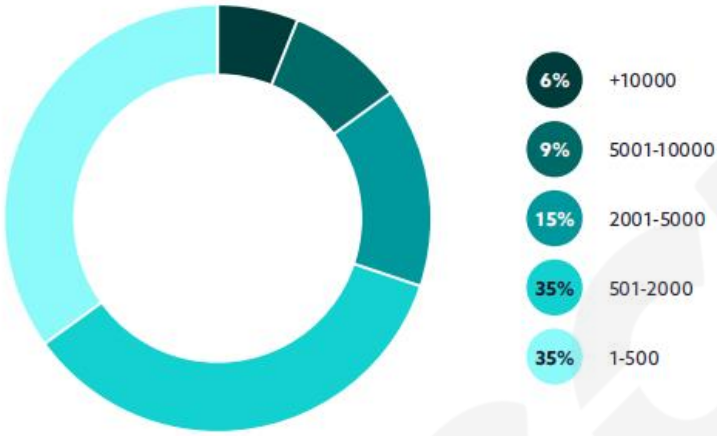


您个人位于哪个区域？

您的组织机构属于以下哪个行业？



您的组织机构有多少员工？



您在组织中属于下面哪个角色 ？