ivanti

远程
居家工作
网络安全
报告

2020

概览

安全访问解决方案提供安全的远程计算，把人员和设备连接到数据中心和云应用，从而保障企业运行——即使是在最不可预测的情况下。

随着新型冠状病毒（COVID-19）疫情加剧并最终演变为一场大流行，世界卫生组织建议人们在家工作，避免使用公共交通和办公室，以避免和减缓疾病传播和感染风险。

2020年初，全球各地的政府和地方官员均开始建议或要求居民居家避疫，除了必要行业人员外，停止外出上班。 各企业也立即采取行动，扩大远程居家工作（WFH）的范围并提供便利。

紧急的工作空间转变和对远程工作能力的急迫需求，不仅可能影响用户的工作效率，还对IT基础架构、业务连续性和信息安全带来了威胁。

这份由Pulse Secure赞助、Cybersecurity Insiders推出的《2020年远程居家工作报告》深入探索企业实现员工和资源过渡的过程，并挖掘了与WFH网络安全相关的挑战、顾虑、战略和预期结果。 调查于2020年5月进行，400多名受访者来自多个行业，包括IT安全决策者、从业者和大小公司。调查发现，84%的公司预计会有更广泛和永久性的远程工作规划，而近三分之一的公司计划在短期内增加安全访问的预算。

主要发现包括：

- WFH用户容量扩大了3倍以上，超过75%的企业的远程工作率达到了近100%
- 33%的企业对紧急远程安全访问的准备不够充分
- 54%将加速将更多的工作流程和应用程序转移到云端
- 38%获得了工作效率的提高和其他好处
- 84%预计会有更广泛和永久性的WFH计划
- 超过半数预计会在未来12个月（2020年4月之后）增加安全访问预算
- 66%预计WFH的安全威胁会增加，而63%预见到WFH可能会造成合规风险
- 恶意软件、网络钓鱼、未经授权的用户和设备访问以及未打补丁的系统被视为最常用的WFH攻击向量
- 反病毒/恶意软件、防火墙、SSL VPN、多因素认证和备份是确保WFH安全/业务防御的最常用解决方案

非常感谢Pulse Secure 对这一重要研究项目的大力支持。

我们希望这份报告能为您提供有用信息和帮助，协助您不懈地保护您的IT投资、确保业务连续性、为您的员工提供保障。

谢谢！

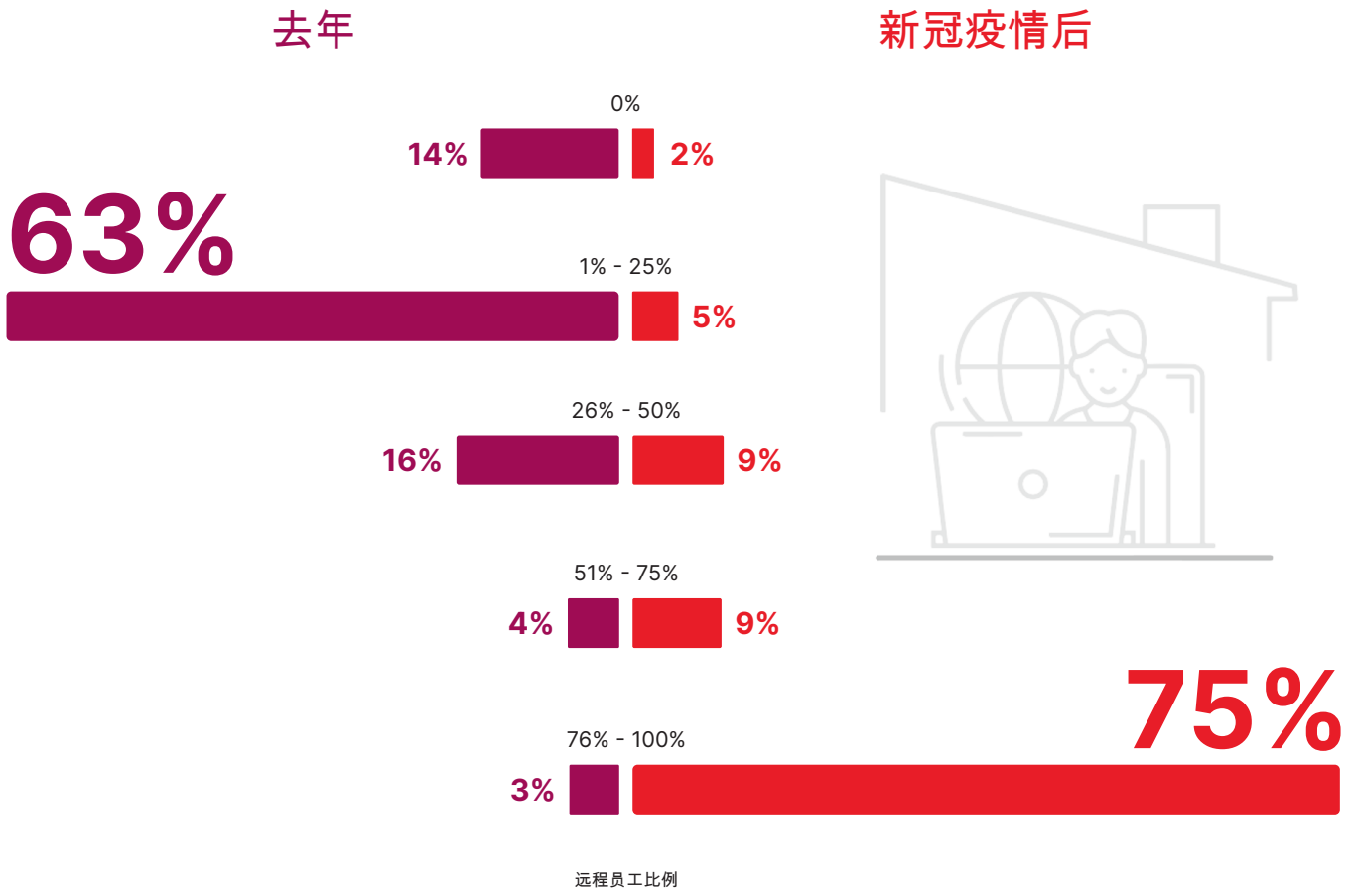
Holger Schulze

Holger Schulze
CEO兼创始人
Cybersecurity Insiders

爆炸式增长的远程工作规模

调查显示，COVID-19新冠疫情促进了大规模的远程和居家的工作环境转型。虽然63%的企业在疫情前已有多达四分之一的员工远程/在家工作，但这些企业目前的居家工作员工比例已达到惊人的四分之三。

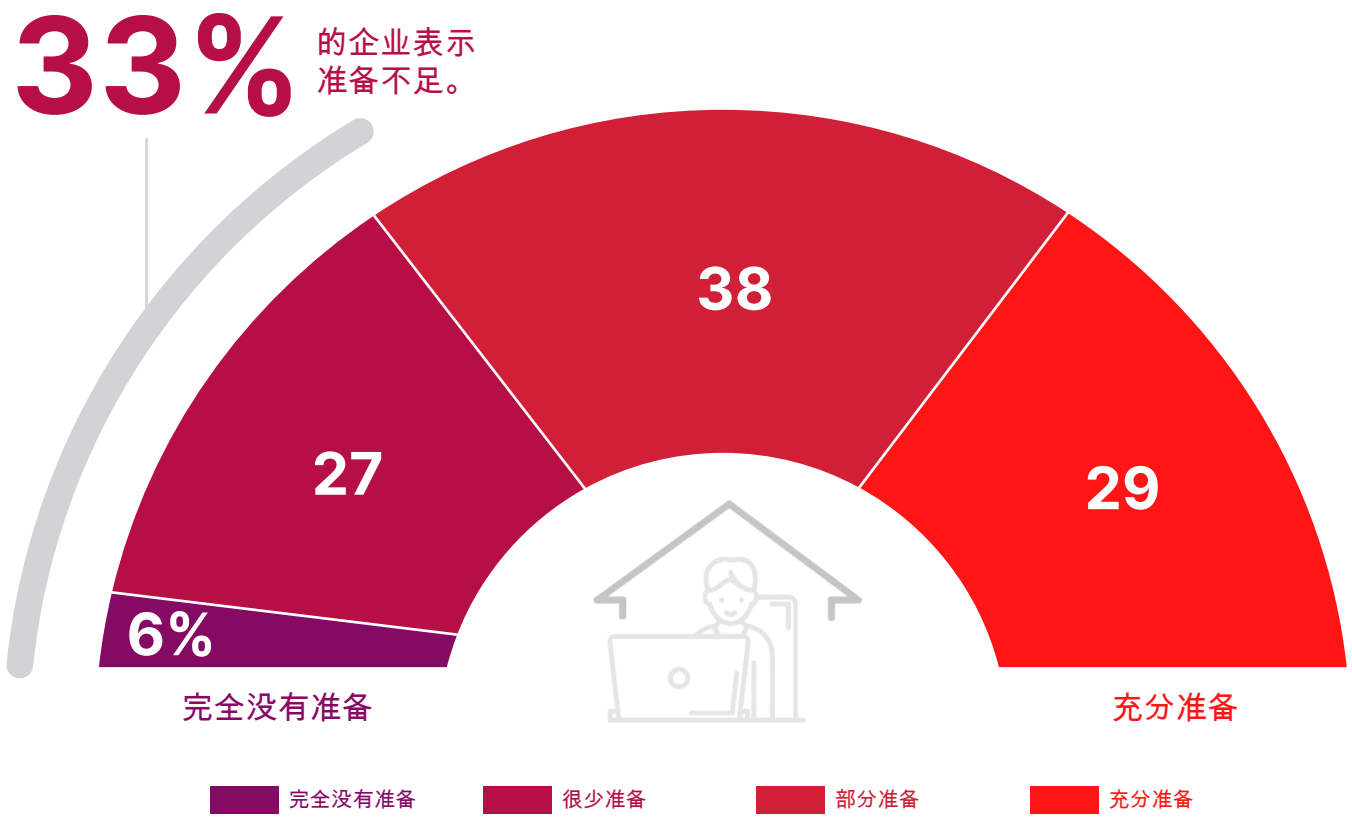
现在（新冠疫情期间）与去年相比，您有多大比例的员工远程/在家工作？



为远程工作所作的准备

三分之一企业表示，他们在面临从实地工作到远程工作的快速转变时准备不足。

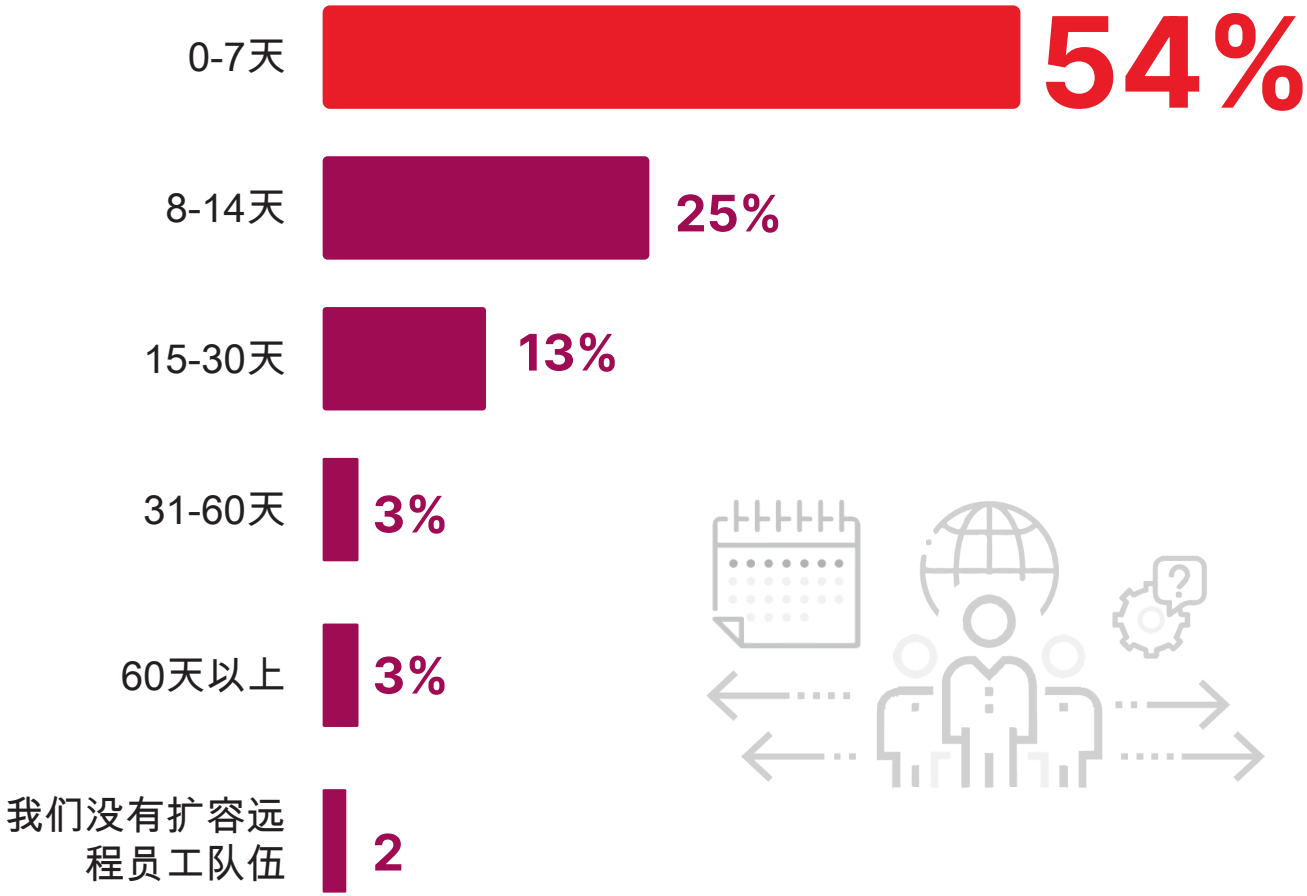
在COVID-19大流行之前，您的企业是否有充分的业务连续性/灾难恢复计划准备，包括迅速从企业内部工作转为远程工作？



扩展远程工作能力所需天数

多数企业（54%）表示，他们在七天或更短的时间内成功地扩展了能力，可全面支持增加的远程员工。

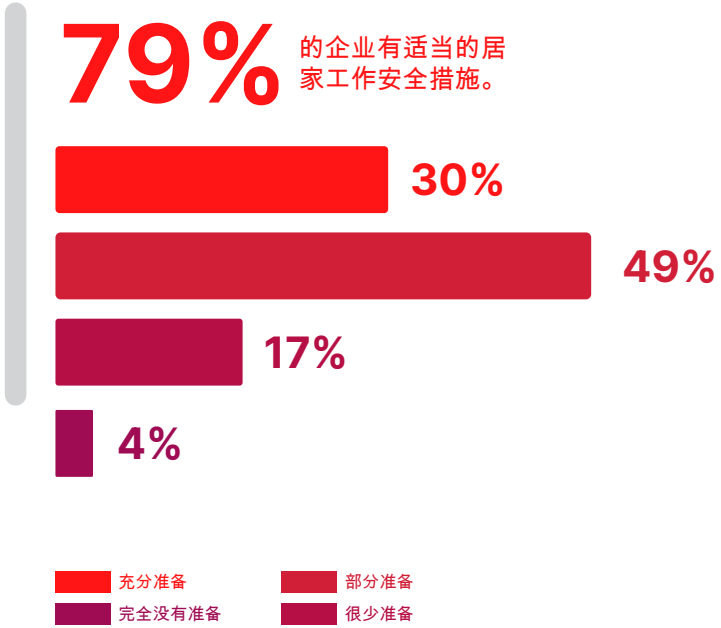
您的企业用了多少天来扩展能力，才能向近期增加的远程员工提供全面支持？

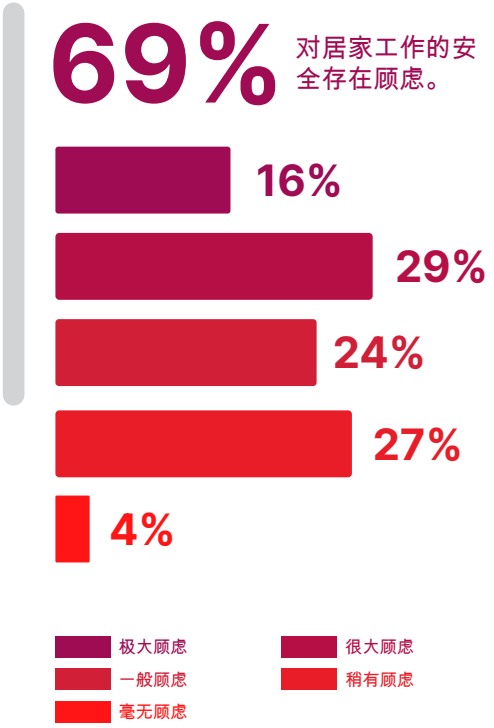


远程工作安全意识

虽然79%的企业认为他们已做好充足的WFH安全准备，本次调查中依然有三分之二（69%）的企业对用户在家工作带来的安全风险表示担忧。

您是否对用户在家工作带来的安全风险感到担忧？从安全角度分析，您的企业是否已对远程工作的转变作好准备？





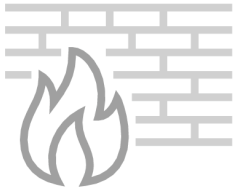
安全控制部署情况

为保护远程工作/居家工作，最常用的安全控制措施是防病毒/防恶意软件解决方案（77%）、防火墙（77%）、虚拟私人网络（66%）和多因素认证（66%）。

您目前部署了哪些安全控制措施来保护远程工作/居家办公环境？

77%

防病毒/防恶意软件



77%

防火墙

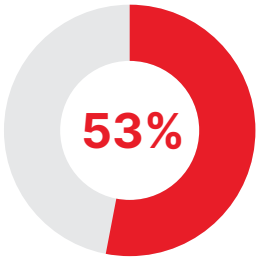
66%

虚拟专用网络
（VPN/SSL-VPN）。

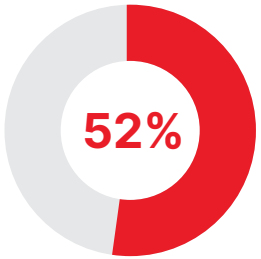
66%

多因素验证
（MFA）

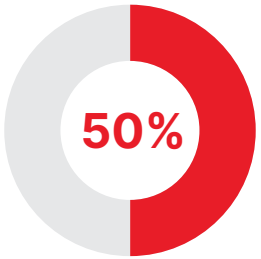
反钓鱼 47% | 单点登录 45% | 端点合规 34% | 移动设备管理 (MDM) 34% | 网络应用防火墙 (WAF) 29% | 虚拟桌面基础架构 (VDI) 26% | 负载均衡/应用交付控制器（ADC） 24% | 网络代理/网络过滤 23% | 云DLP 18%| 云访问安全代理（CASB） 16% | 用户和实体行为监控(UEBA) 11% | 软件定义边界(SDP) 10% | 零信任网络访问(ZTNA) 8% | 其他3%



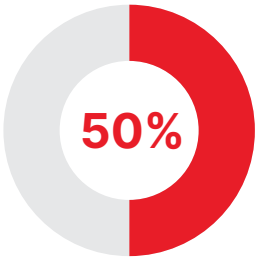
备份和恢复



密码管理



文件加密



端点安全（EDR）

主要安全挑战

对于正在扩容远程工作的企业，用户意识是主要安全挑战中最重要的一项（59%）。紧随其后的是通过家庭或不安全的公共网络访问（56%）和使用个人设备（43%）。

您认为贵公司在扩容远程工作时面临的最大安全挑战是什么？

59%

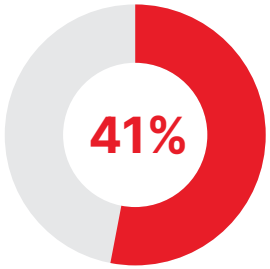
用户意识和培训

56%

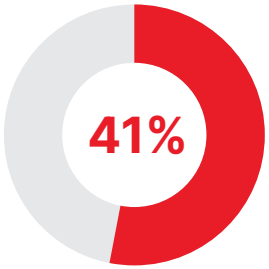
家用/公共WiFi网络安全

43%

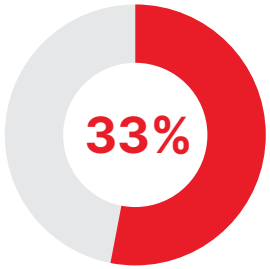
使用个人设备/自有设备



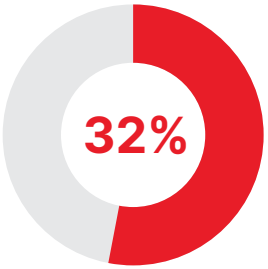
敏感数据流出边界



增加的安全风险



缺乏可视性



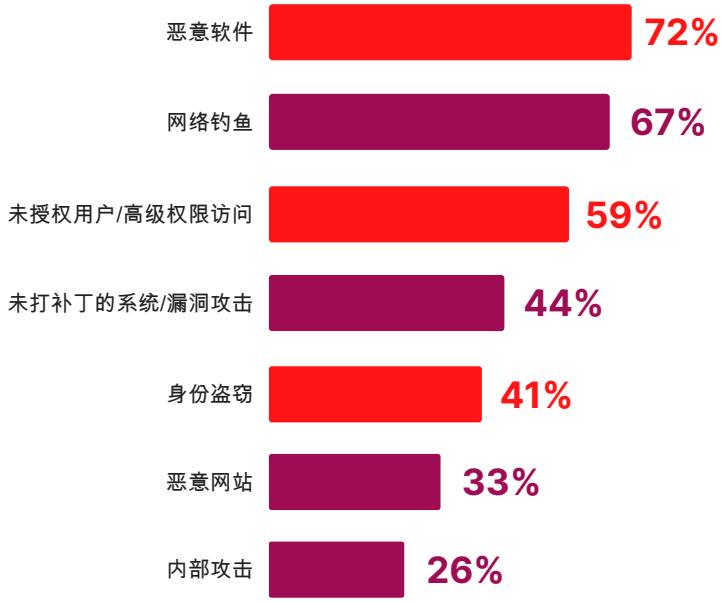
安全解决方案的成本增加

可用性/用户体验 30% | 扩大能力 24% | 不受控制的云端应用使用 21% | 问责/审查缺失 21% | 无 5% | 其他 2%

扩大的攻击向量

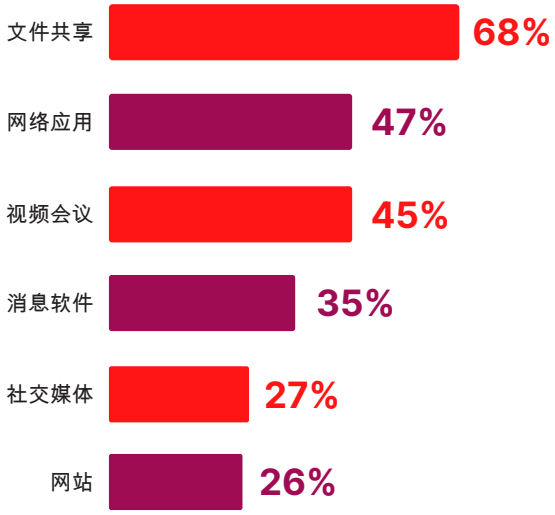
恶意软件、网络钓鱼、未经授权的用户/设备访问和未打补丁的系统被认为是员工居家工作面对的主要攻击向量。而在与工作效率和协作有关的应用程序中，文件共享（68%）、网络应用（47%）、视频会议（45%）和消息软件（35%）为企业带来了最大的安全隐忧。

在员工居家工作的情况下，您最担心的是哪些攻击向量？



其他 5%

在安全方面，远程员工使用的哪些办公应用程序是最让您感到担心的？



其他 2%

远程工作安全水平

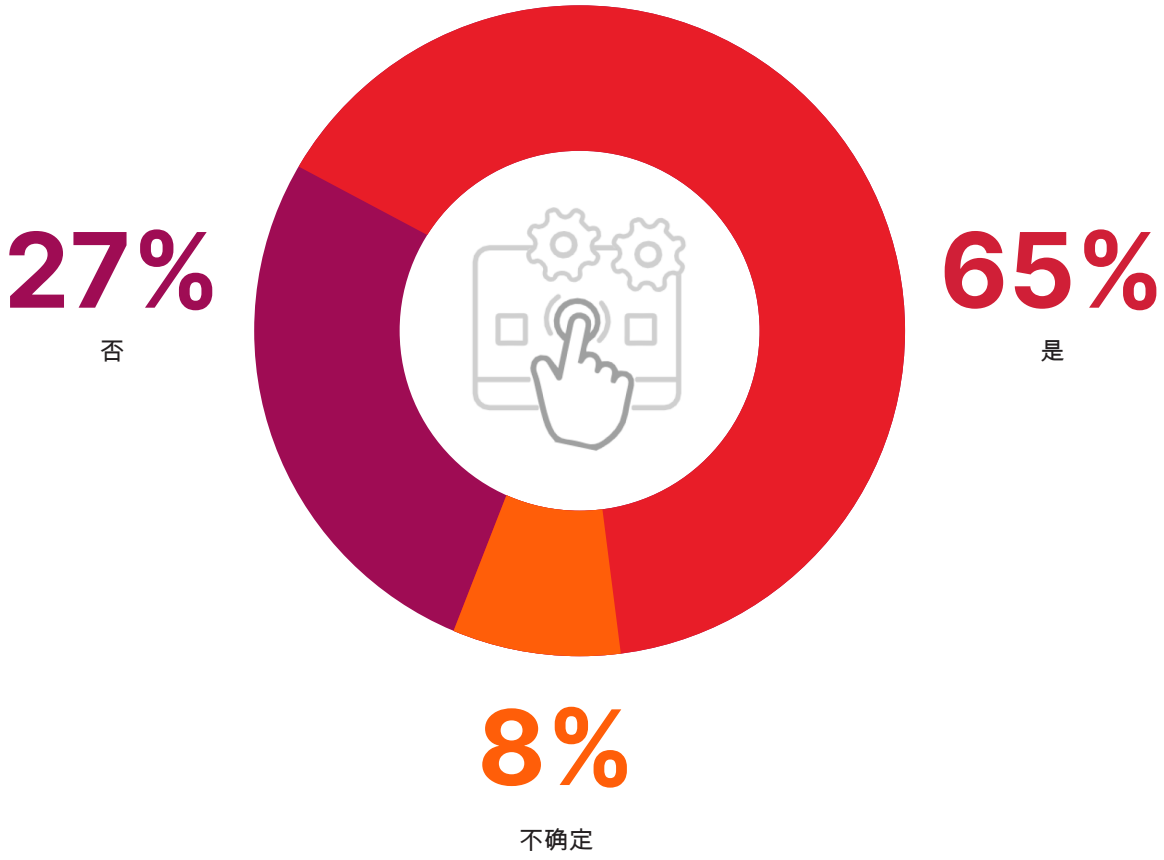
大多数受访者（78%）证实说，他们对所有远程访问的角色均采取相同级别的安全控制。

您是否对远程访问的所有公司角色均执行相同级别的安全控制和数据管理？

使用个人设备发起访问

将近四分之三的企业允许使用不受管理的个人设备在家工作，而其中至少27%认为这种情况会产生重大安全风险。

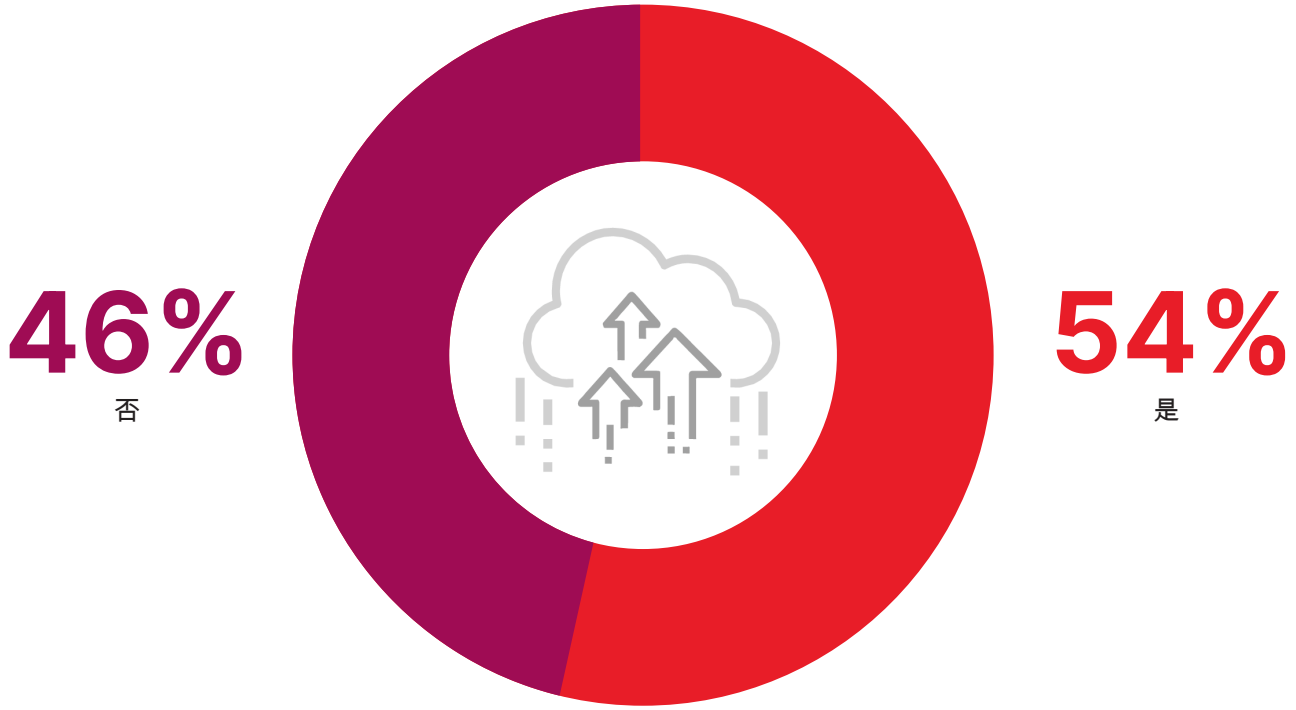
员工是否能够从不受管理的个人设备访问受管理的应用程序？



云迁移

大多数受访者（545）认为，新冠疫情加速了工作流程向云应用的迁移过程。

COVID是否加速了更多用户工作流程或应用程序向云应用的迁移过程？



远程工作安全风险

企业最关心的是保护敏感数据，尤其是在数据被不受管理的端点访问时（46%），其次是暴露于恶意软件的几率增加（34%）。

在您的用户进行远程连接时，您最担心的主要风险是什么？

59%

保护我的数据，尤其是在受到不受管理的端点访问时

56%

暴露在恶意软件、网络钓鱼或其他攻击之下

确保我的受监管用户的合规性

审查和监督使用不受管理的资源工作的员工

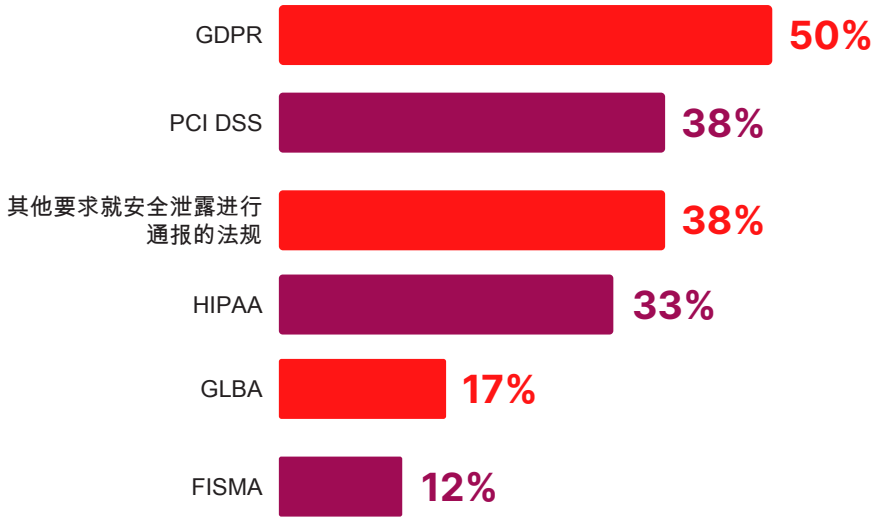
其他 4%

对合规性的影响

三分之二的受访者认为远程工作环境会对企业合规性情况造成影响。

远程工作是否会影响适用于您的企业的合规性要求？

如果是，是哪些？



对工作效率的影响

38%的企业认为，远程工作带来了更高的工作效率和其他优势，只有16%的企业认为效率下降了。

您的企业是否通过远程工作获得了更高的工作效率和其他优势？

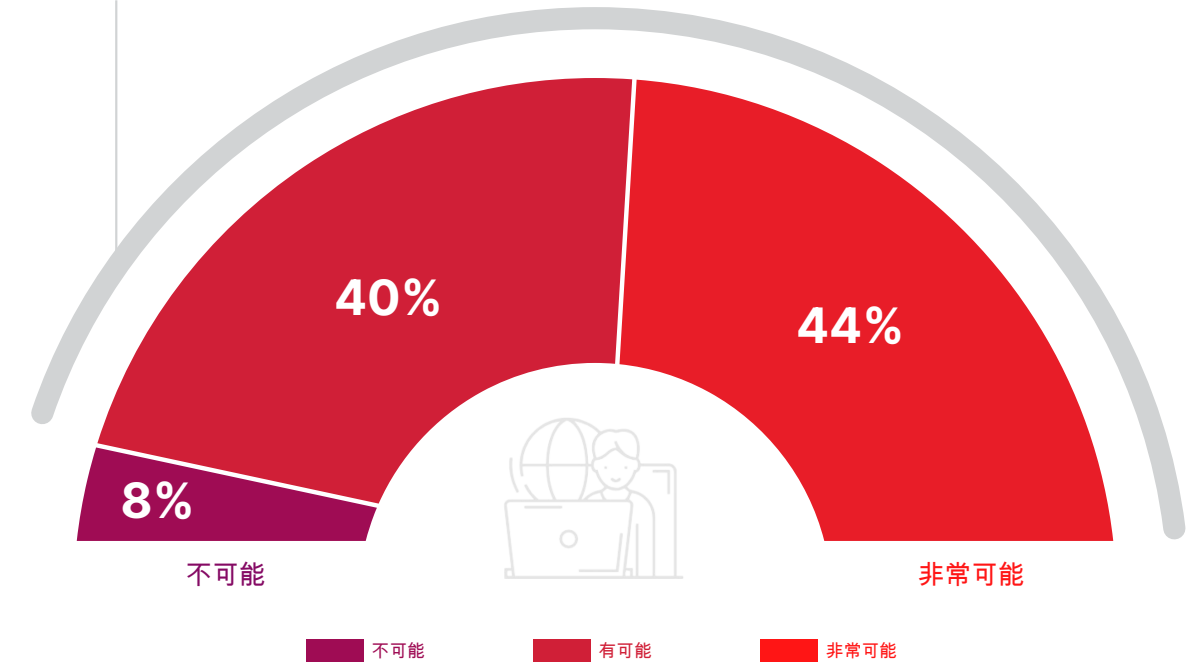
38% 获得了更高的工作效率和其他远程工作带来的优势。

未来的远程工作

84%的企业认为有可能（44%非常有可能）在未来继续扩大居家工作的能力，从而享受更高的工作效率和其他业务优势。

你是否认为会在未来继续支持扩大居家工作能力（基于更高的工作效率和其他业务优势）？

84% 的企业认为有可能在未来继续扩大居家工作的能力。

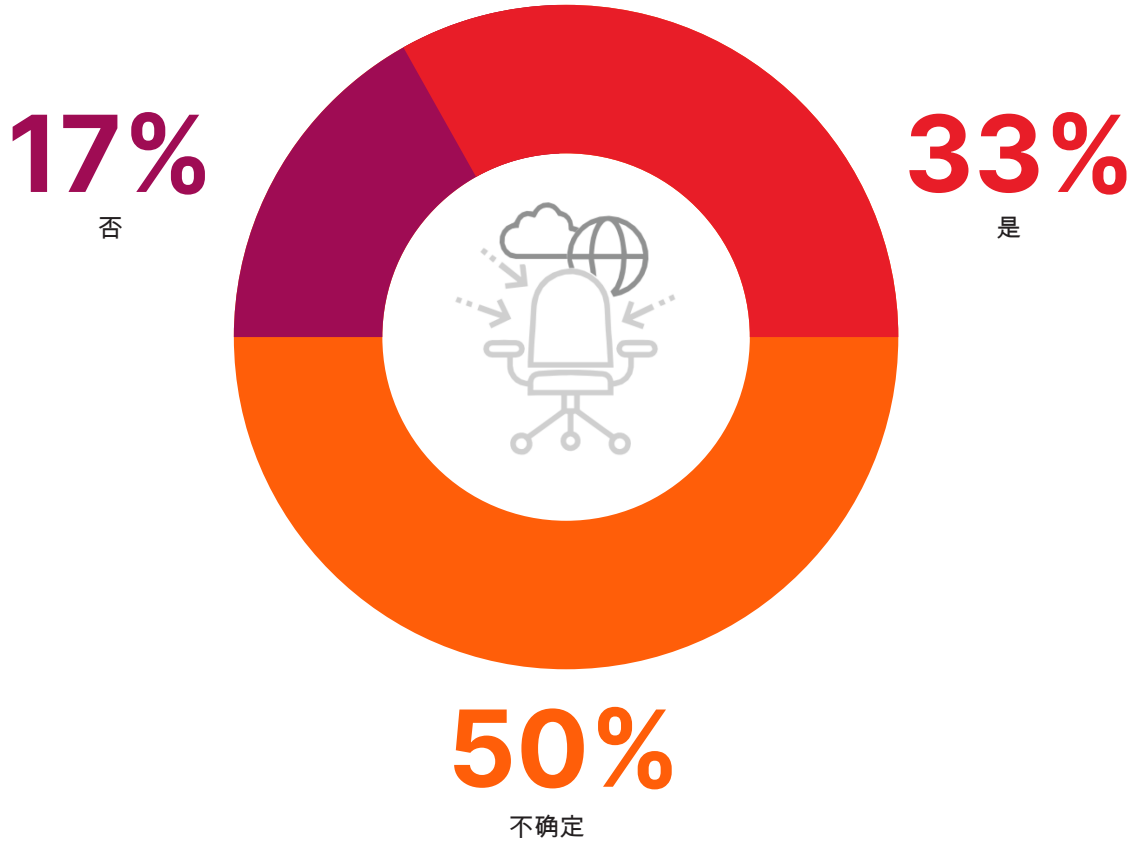


不确定 8%

远程工作常态化

三分之一的企业正在考虑在新冠危机结束后把一些职位永久转为远程工作。

您的企业是否正在考虑在新冠危机结束后，把一些职位永久转为远程工作（之前是驻场工作）？

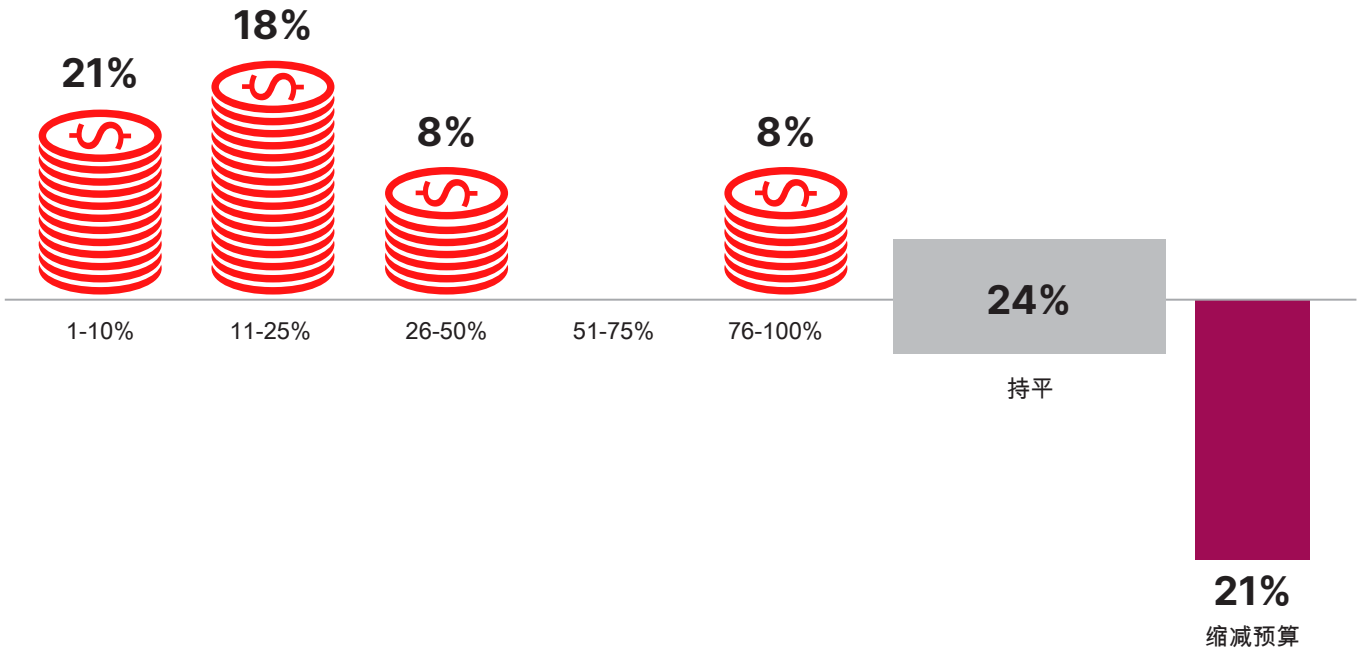


预算趋势

多数（55%）企业预计在未来12个月（2020年4月以后）增加用于远程员工安全的预算。而四分之一的受访者表示相关预算将持平，只有21%认为预算会缩减。

在未来12个月内，您的远程工作安全控制预算是否会增加？

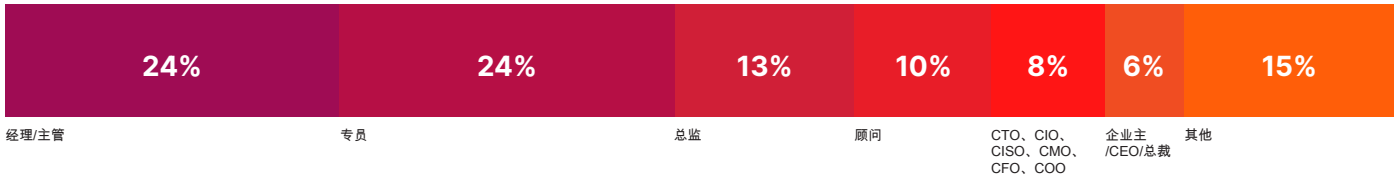
55% 认为未来12个月内的远程工作安全预算会增加。



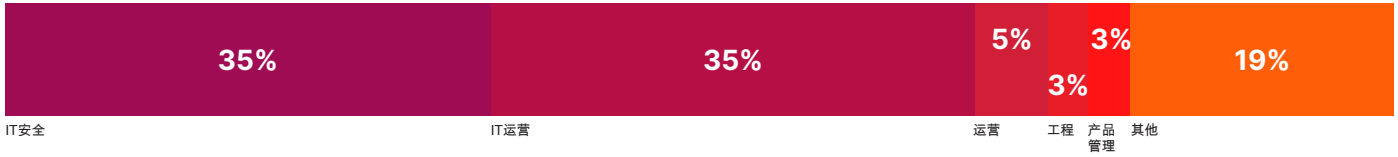
研究方法&人群统计资料

本报告基于一项全面网上问卷调查的结果，该调查于2020年5月在美国进行，共访问了413位IT和网络安全专业人士，目的是研究企业在2020年新冠疫情中在远程工作方面的最新采用趋势、挑战、空白和解决方案选择。受访者中有技术主管，也有IT安全从业人员，均衡地代表了多个行业不同规模企业的横截面。

职务级别

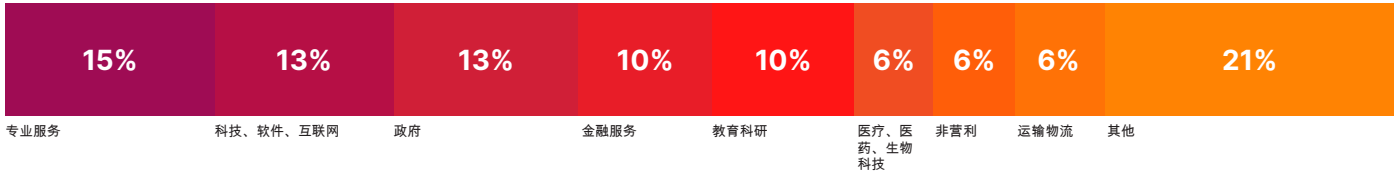


部门



公司规模

行业



Pulse Secure
Acquired by Ivanti

Pulse Secure针对人员、设备、物品和服务提供简单全面的软件驱动安全访问解决方案，从而为客户提升可视性、保护力和工作效率。我们独有的软件套件整合了云端、移动、应用程序和网络访问，在零信任环境里打造混合式IT。已有来自各个垂直领域的23000多家企业和服务提供商信任Pulse Secure为移动员工实现数据中心和云端应用程序和信息的安全访问，同时确保业务合规性。进一步了解请访问 www.ivanti.com.cn。

ivanti

www.ivanti.com.cn
+86 (0)10 85412999
ContactChina@ivanti.com