ivanti PULSE

亚太和日本地区安全访问现状报告

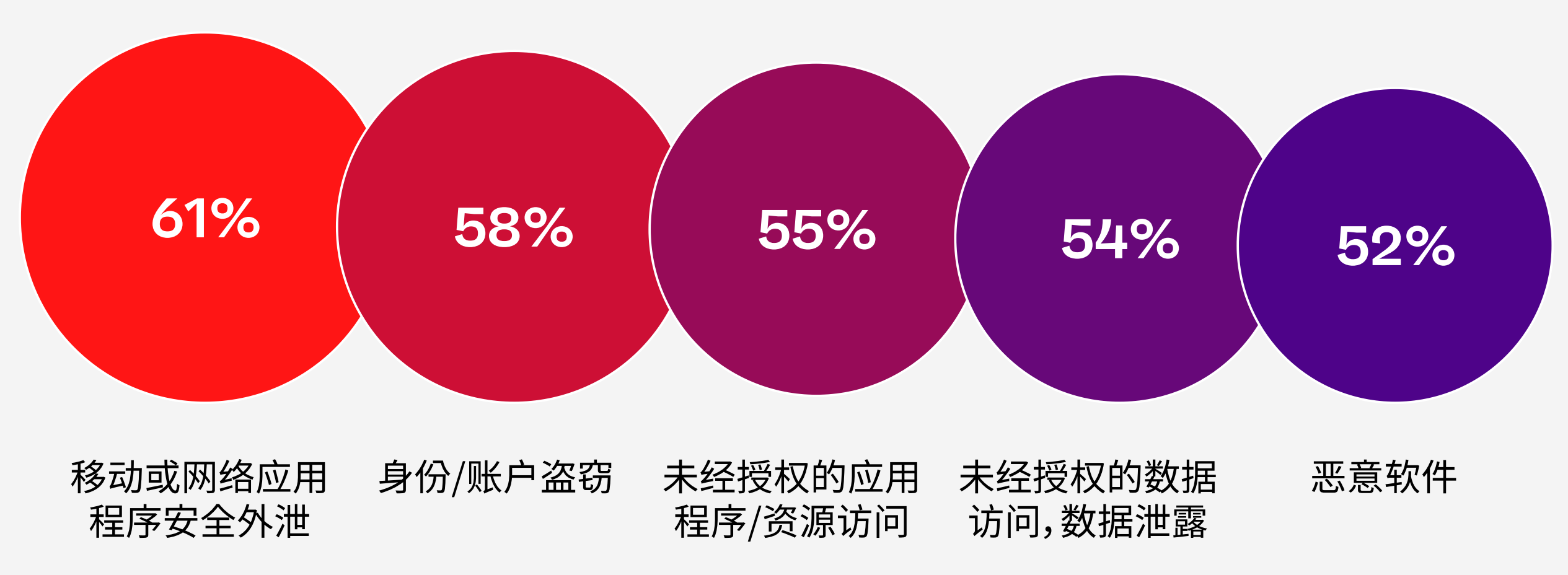
在过去的12个月里，亚洲、太平洋和日本（亚太和日本）地区的安全和IT领导者遭遇了一系列的安全威胁。为了应对这类日益增长的挑战，他们正在着重策划安全访问措施，并有计划接轨零信任协议。然而，不同的行业（软件、金融服务和制造业）的具体优先事项也有所不同。

Ivanti和Pulse调查了亚太和日本地区的125位IT和安全领导者，以了解他们在未来12个月中的安全访问重点，探讨如何通过安全访问措施降低安全威胁的频率。

企业需要定义访问策略来对抗安全威胁

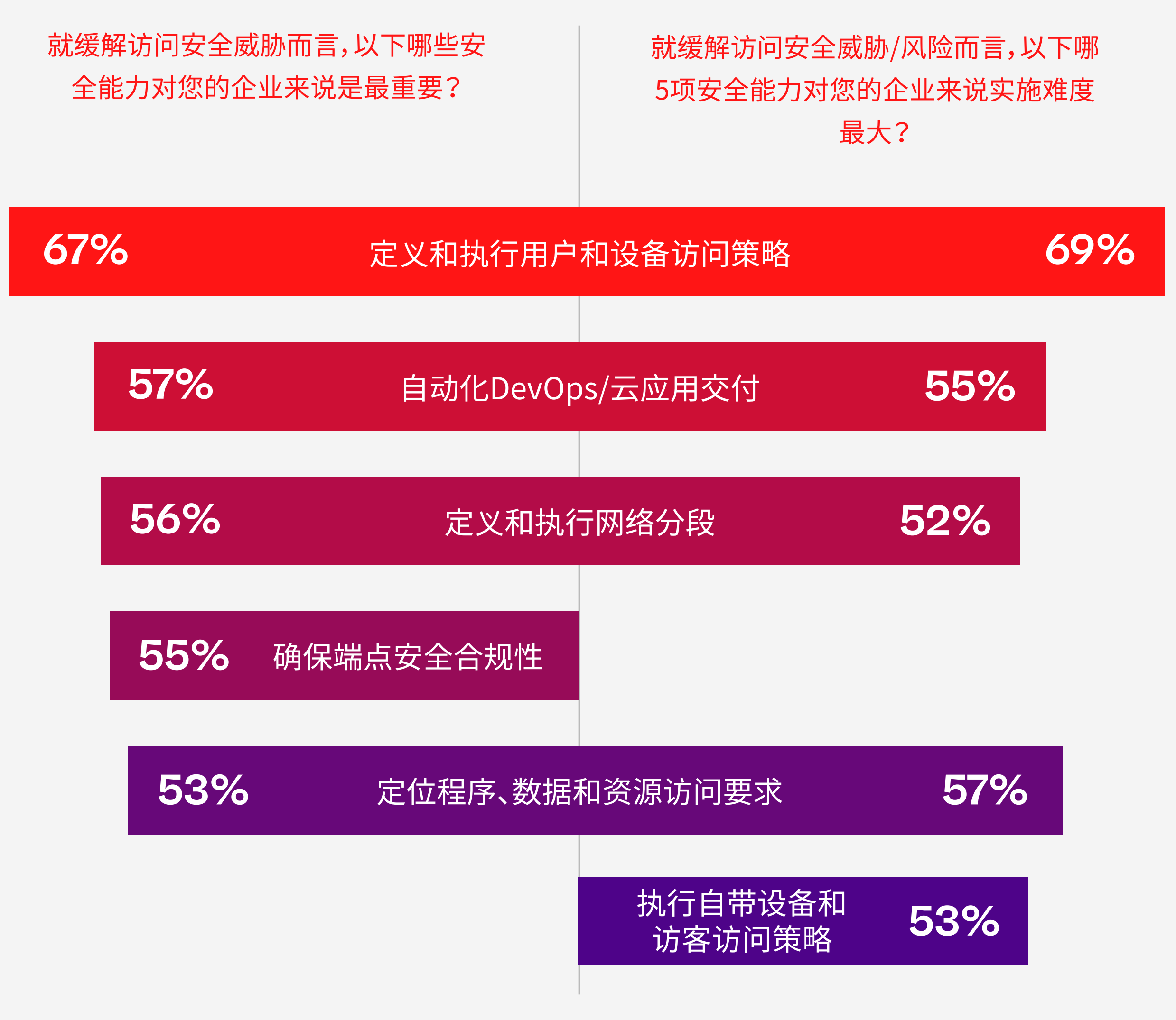
在过去的一年里，超过半数的亚太和日本地区公司曾遭到安全攻击。受访的IT和安全领导者所属的企业最经常遇到的是移动或网络应用程序安全外泄（61%）、账户欺诈和身份盗窃（58%）以及未经授权的应用程序/资源访问（55%）。

以下5种安全威胁中，哪一种在过去12个月中对您的企业造成了最大影响？

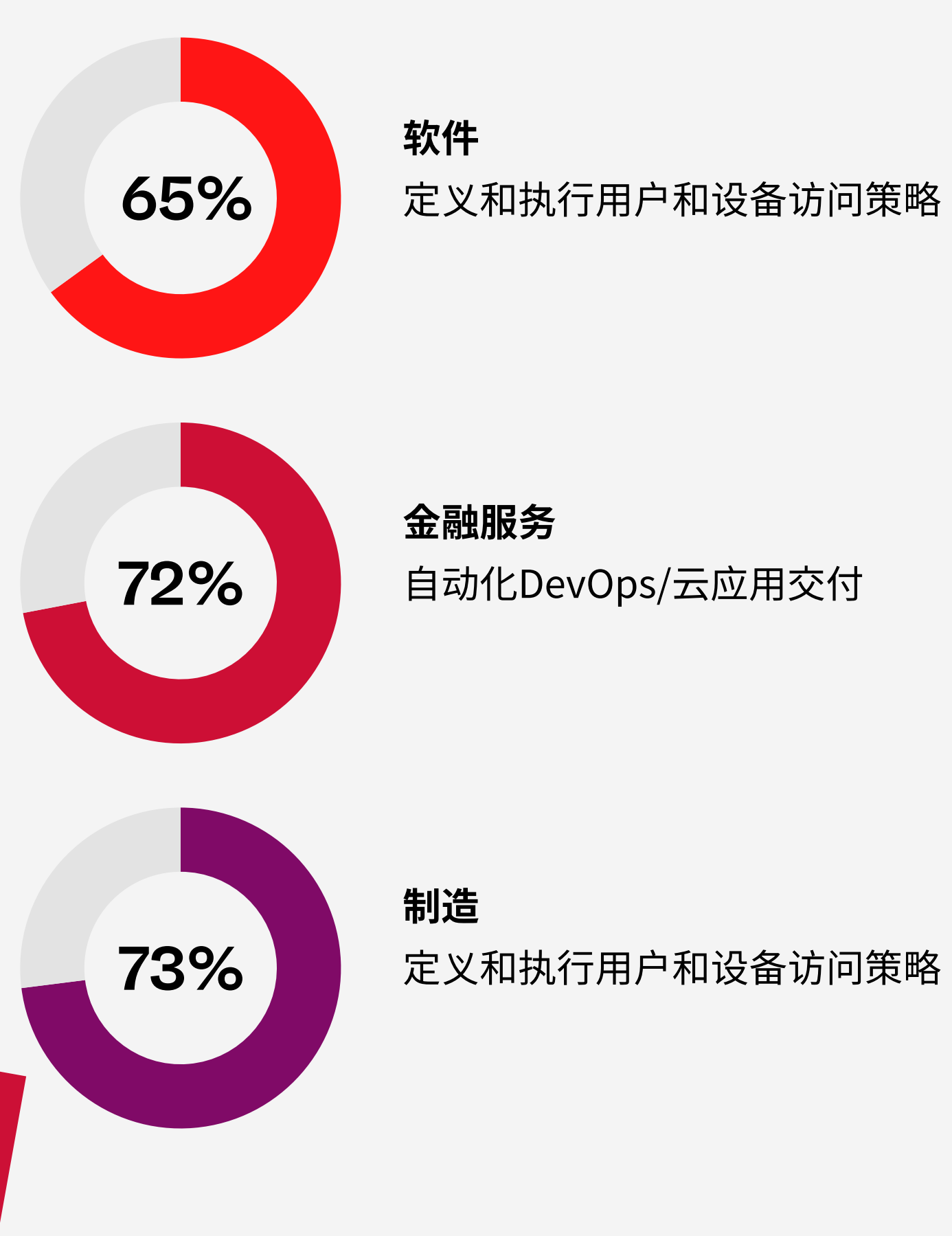


相反，在北美最常见的安全威胁是恶意软件（51%），而欧洲则是未经授权的应用程序/资源访问（70%）。

为了减小这类愈演愈烈的安全威胁的影响，67%的IT和安全领导者表示其企业最需要的是定义和执行用户和设备访问策略。然而，在最重要的5项举措中，有4项同时也是实施难度最大的4项。



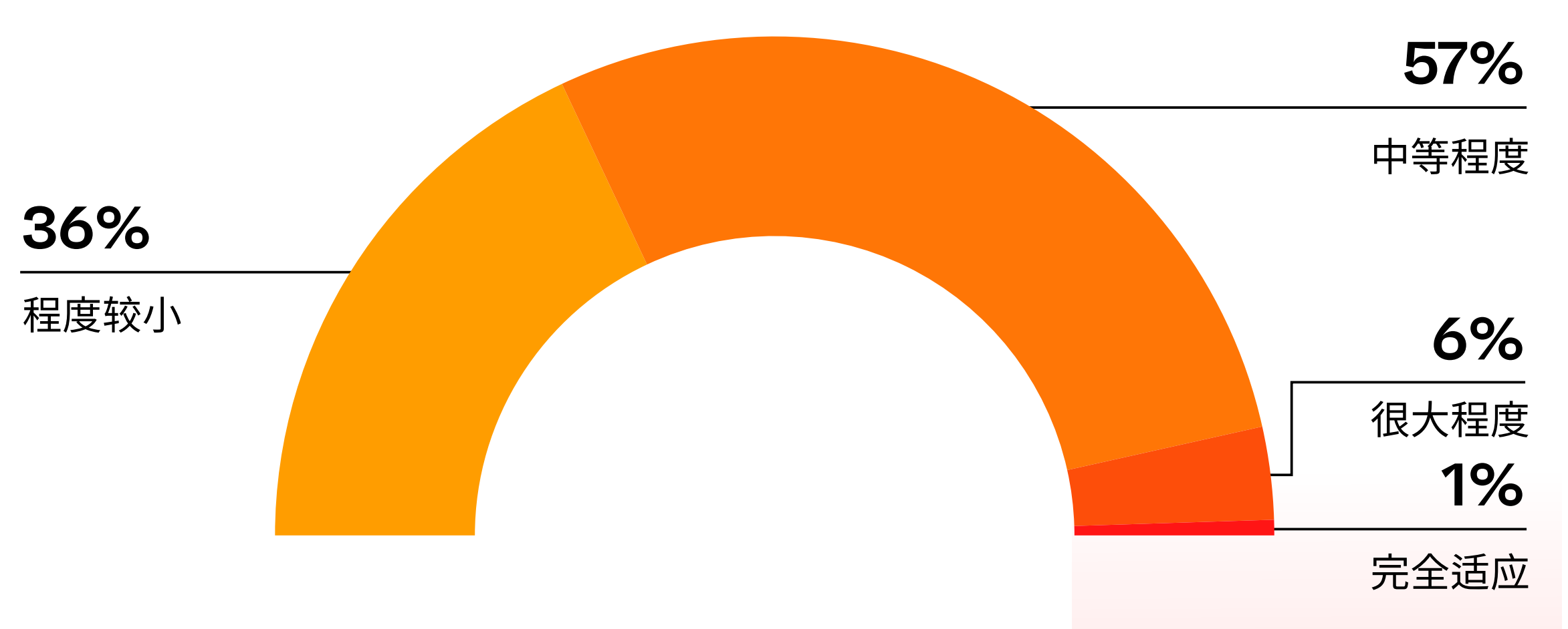
各个行业最需要的威胁缓解能力是什么？



为了进一步防御安全威胁，科技领导者正在优先考虑“零信任”和混合型IT的安全保障

所有（100%）的亚太和日本地区IT和安全从业人员一致表示，其企业的安全操作将在未来12个月内进一步适应零信任策略。

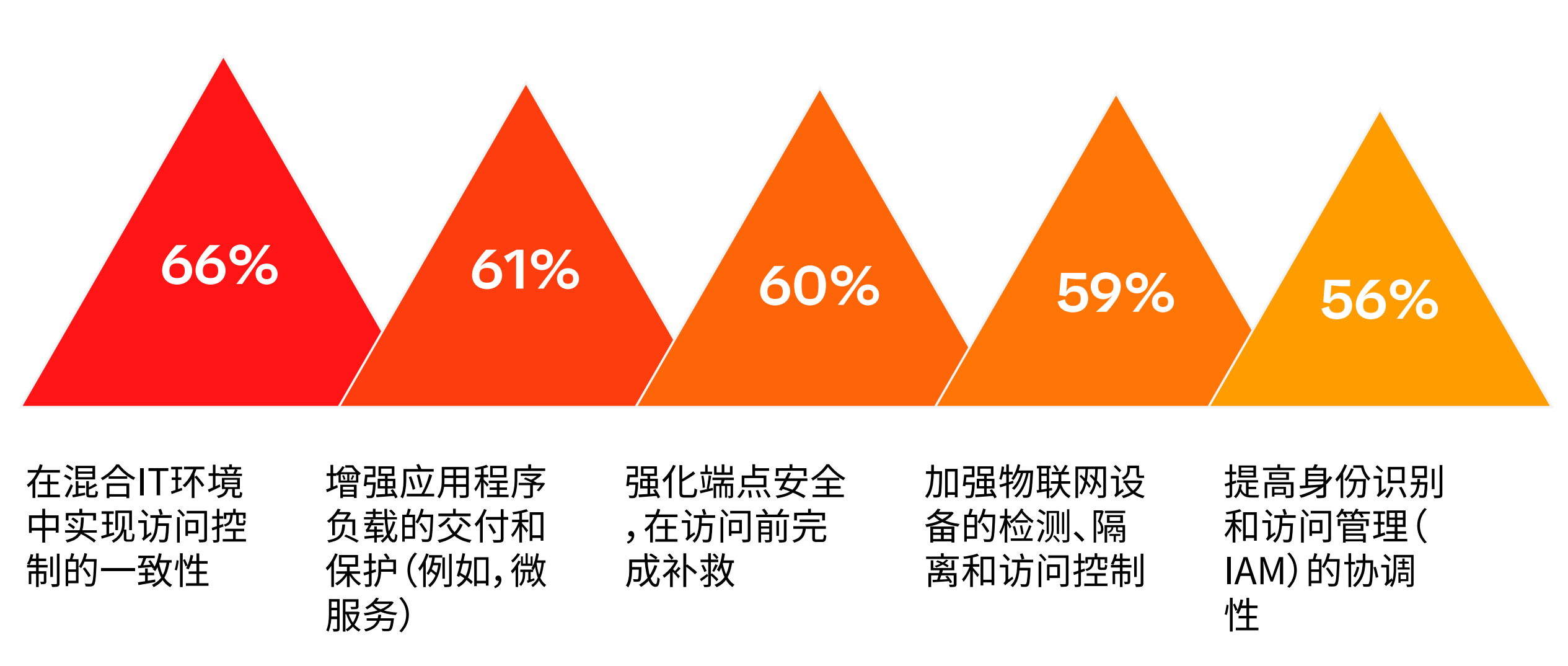
在未来12个月内，您的企业现有的安全控制措施将在多大程度上更加适应零信任策略？



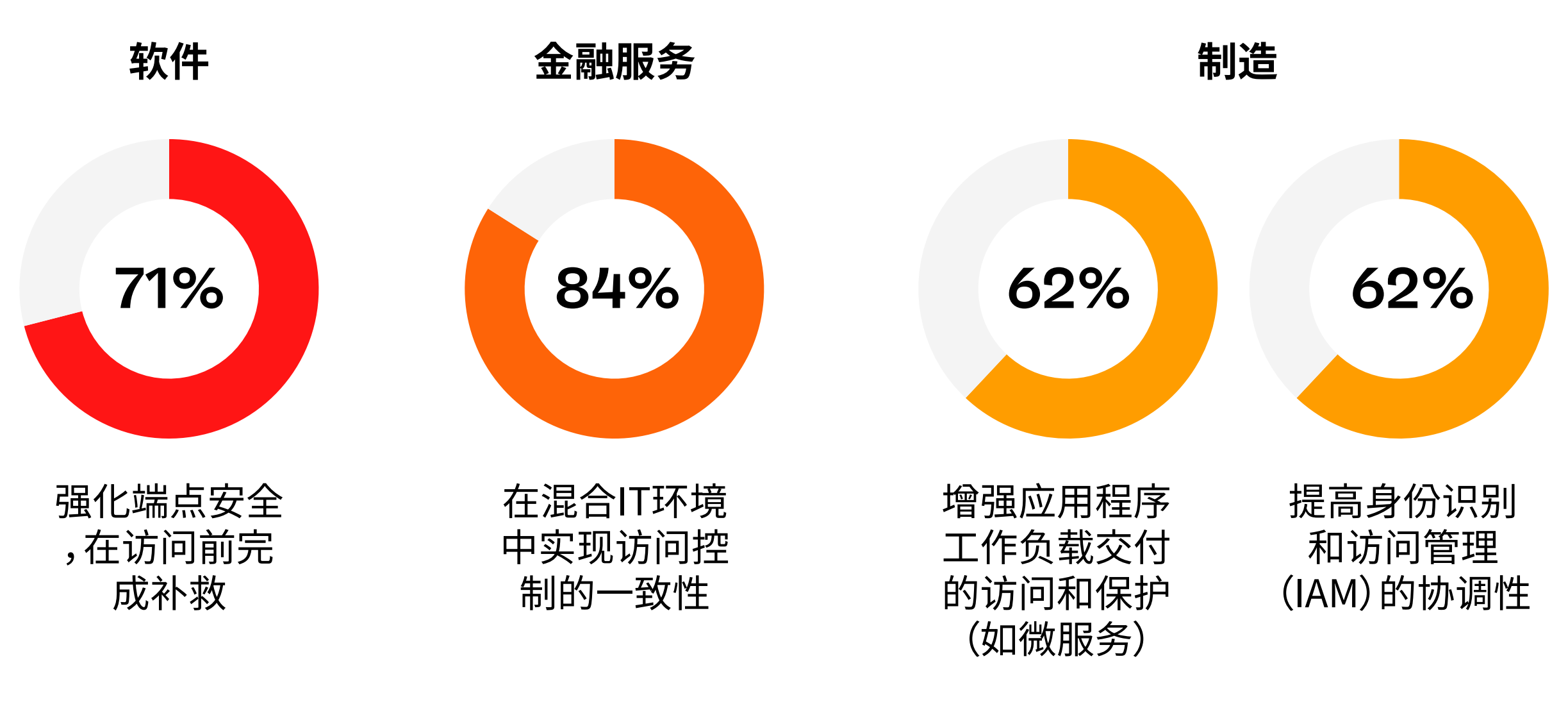
与亚太和日本地区相比，北美地区更重视与零信任接轨。21%的西方国家IT和安全领导者表示，他们将在未来一年内在很大程度上或完全接轨零信任，亚太和日本地区的这一比例只有7%。

各位IT和安全领导者均表示，他们的企业正在重点规划的访问安全措施是为了在未来12个月内实现混合环境中的访问控制一致性（66%），以及增强应用程序负载的交付和保护（61%）。

在未来12个月内，哪些访问安全措施对您的企业来说最重要？



各行业的首要安全措施：



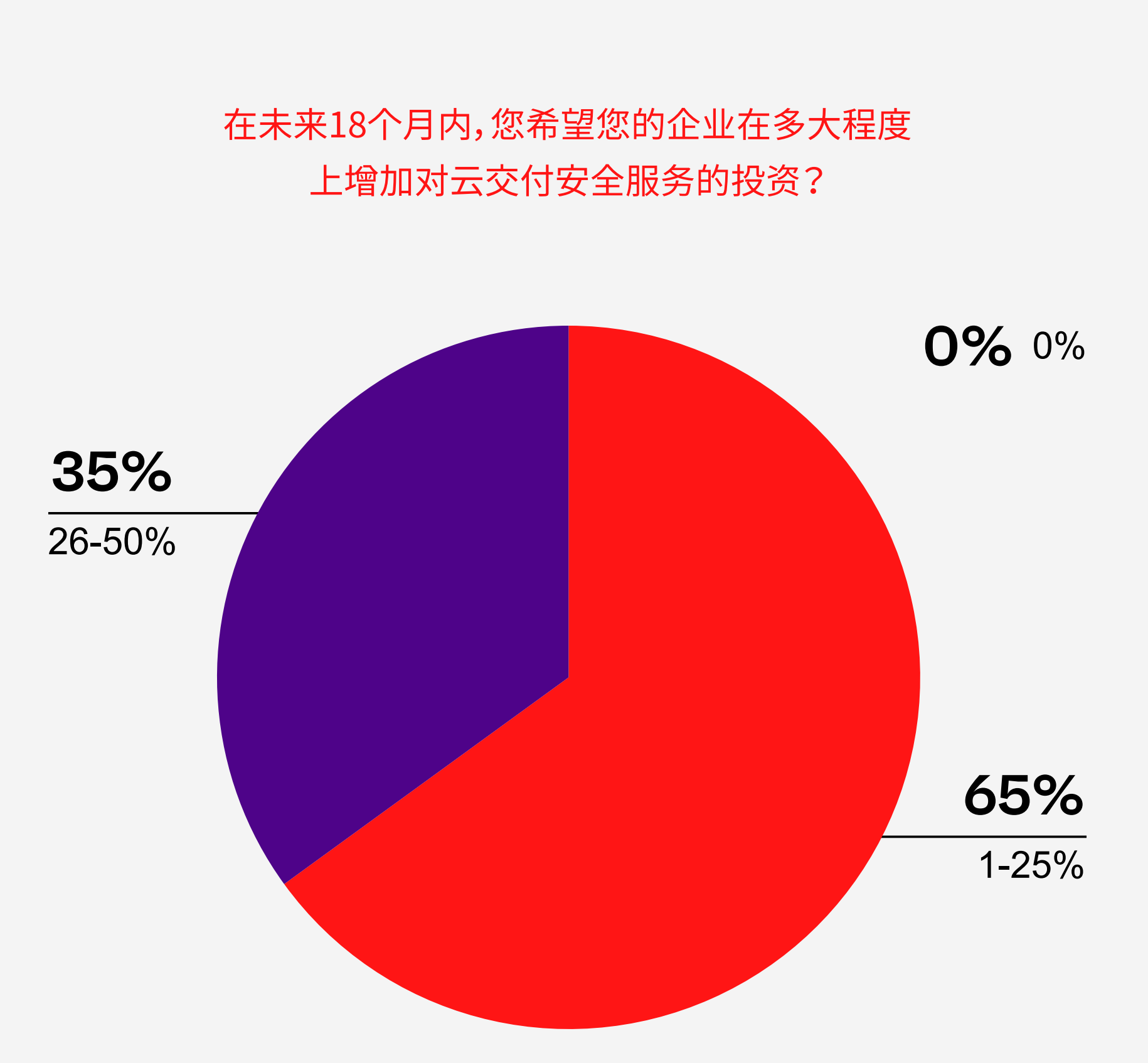
与其他地区相比，亚太和日本地区企业更多地依靠云交付的安全服务，并有计划对供应商进行整合

95%的亚太和日本地区IT和安全领导者表示，他们的企业已有超过四分之一的安全服务过渡到了云交付。

您的企业有多少安全服务已从传统的内部安全工具过渡为云交付？

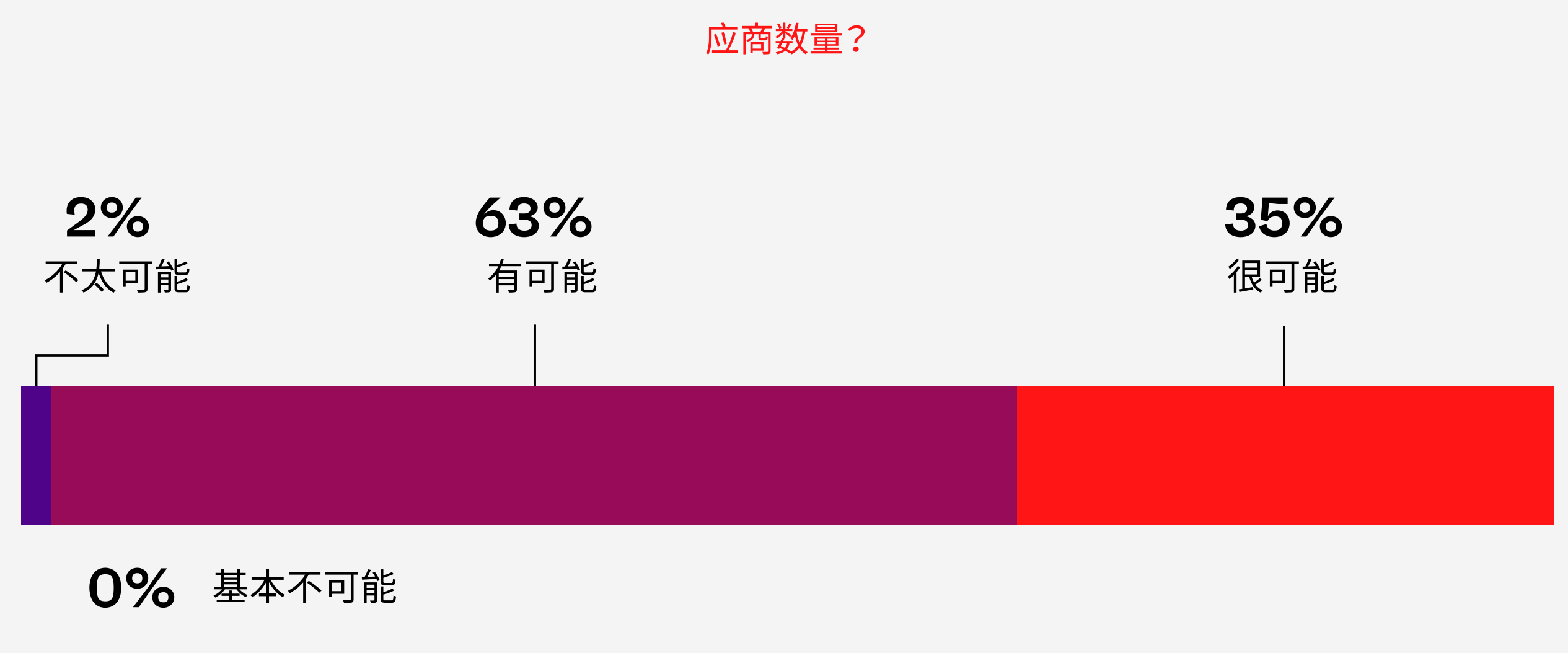
此外，超过三分之一（35%）的人预计其企业明年的云交付安全服务支出将增加25%以上。亚太和日本地区的受访者中无人认为此项预算会维持不变。

在未来18个月内，您希望您的企业在多大程度上增加对云交付安全服务的投资？



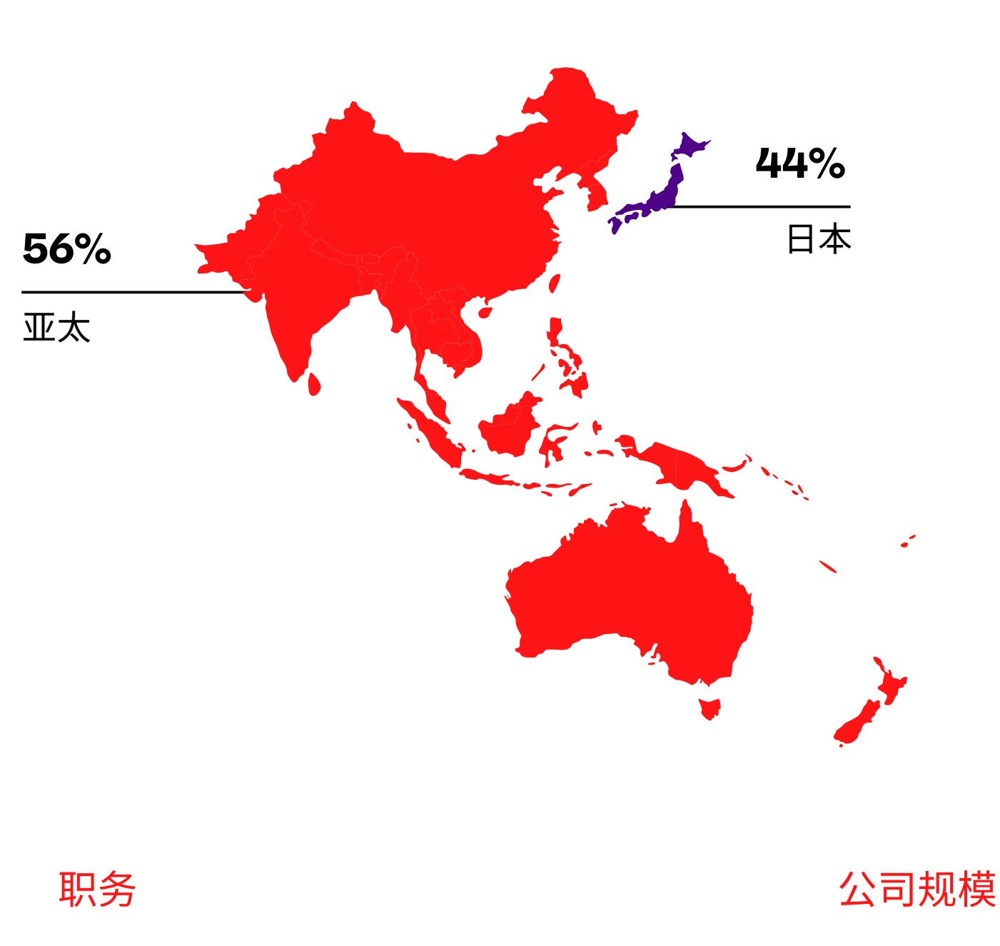
最后，绝大多数受访者（98%）要么正在把安全供应商整合至统一平台，要么有计划在未来几个月内这样做。

在未来12个月内，您的企业有多大可能把独立的安全访问工具整合到更统一的平台，并减少供应商数量？

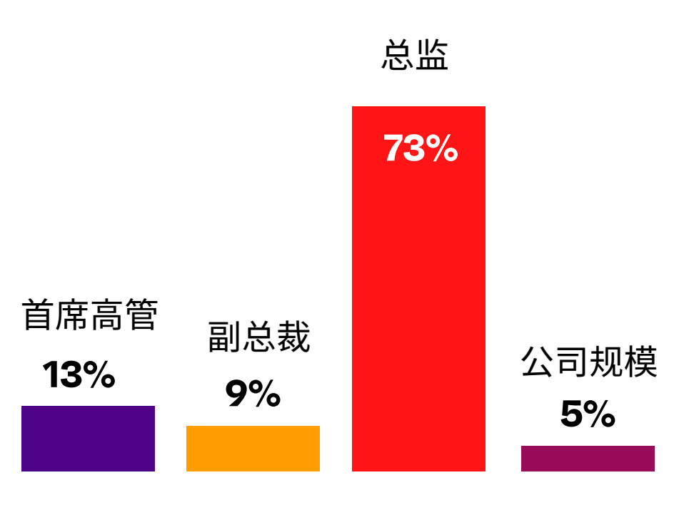


受访者详情

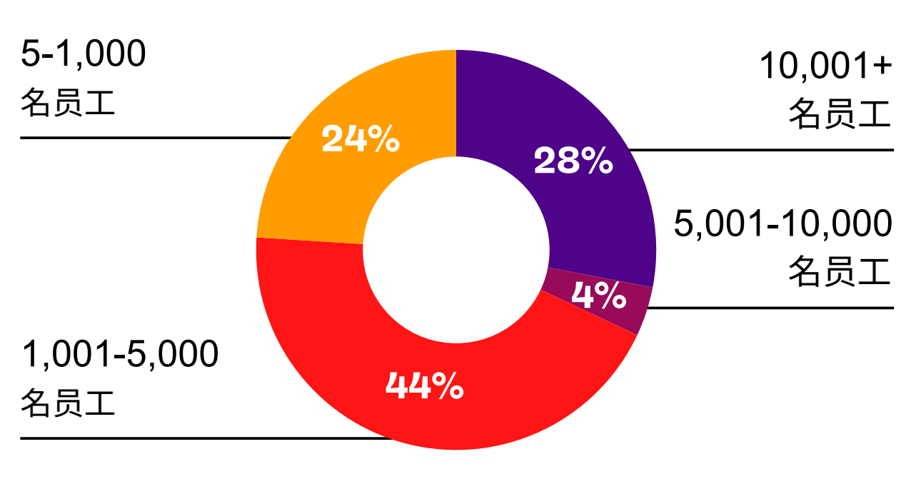
地区



职务



公司规模



数据采集时间：2020年10月1日至11月23日

受访者： 225位IT和安全领导者

PULSE 洞见