aruba
a Hewlett Packard Enterprise company

弥合 IT 安全缺口：

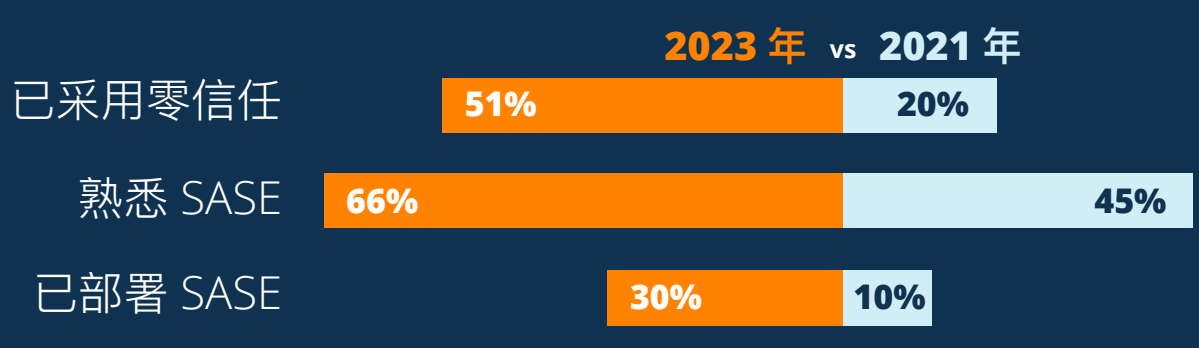
2023 年零信任与 SASE 安全性架构现状

日渐普及的混合工作模式和 IoT，以及无休止的网络攻击，让组织面临着严峻程度远超以往的安全挑战。这些新挑战正在推动新型安全模式的采用。零信任与 SASE（安全接入服务边缘）架构有望：

- 构筑覆盖边缘到云的安全防线
- 以动态方式强制实施资源的最低访问权限策略，进而降低网络风险
- 确保随时随地安全访问企业应用

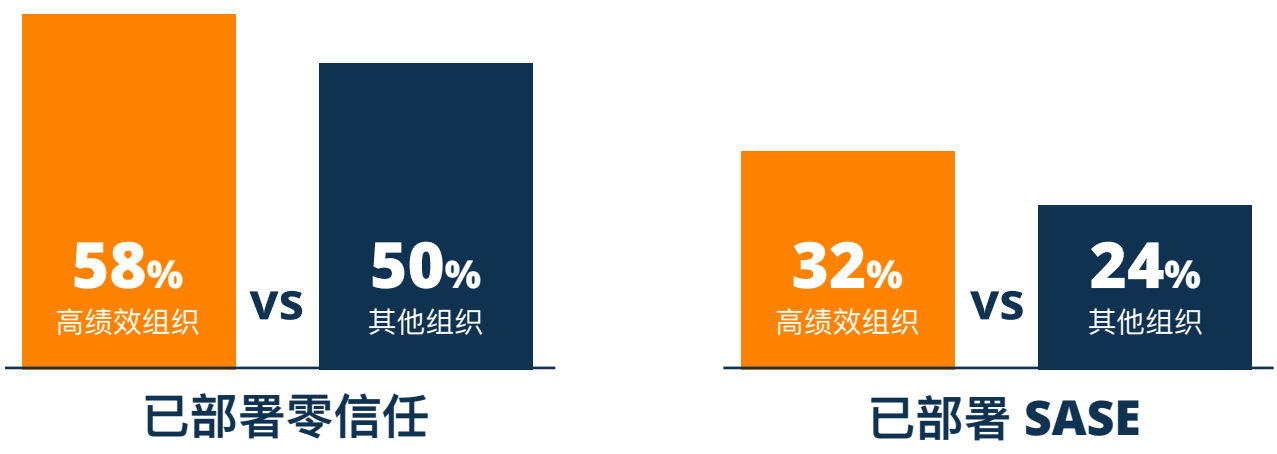
安全性架构正在发生怎样的变化？

过去两年，零信任与 SASE 安全架构的采用速度不断加快。您是否走在前沿？



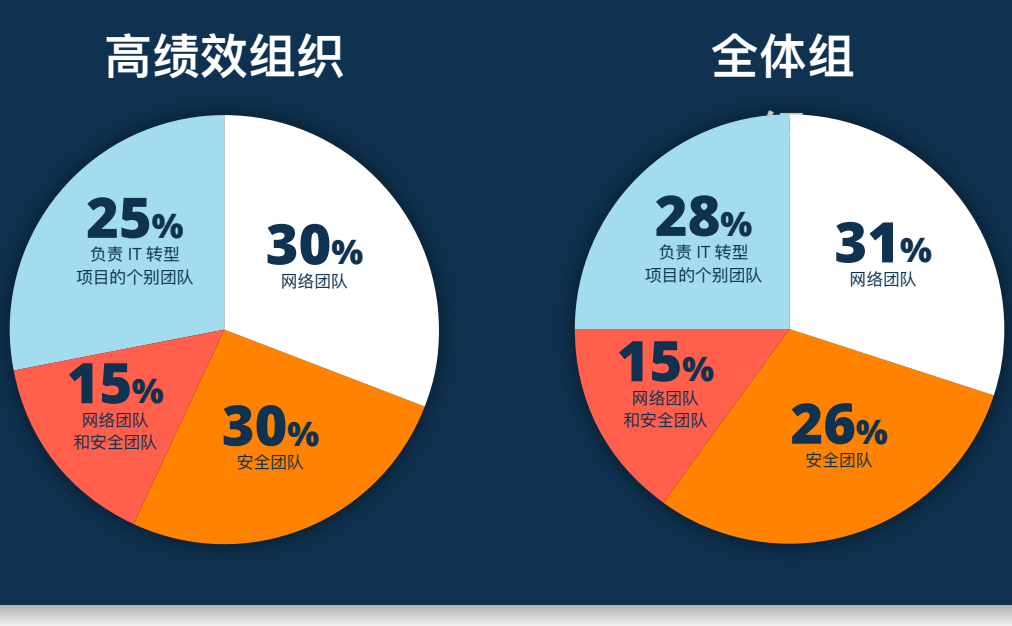
高绩效组织有何独到之处？

高绩效组织部署零信任与 SASE 架构的意愿更高。



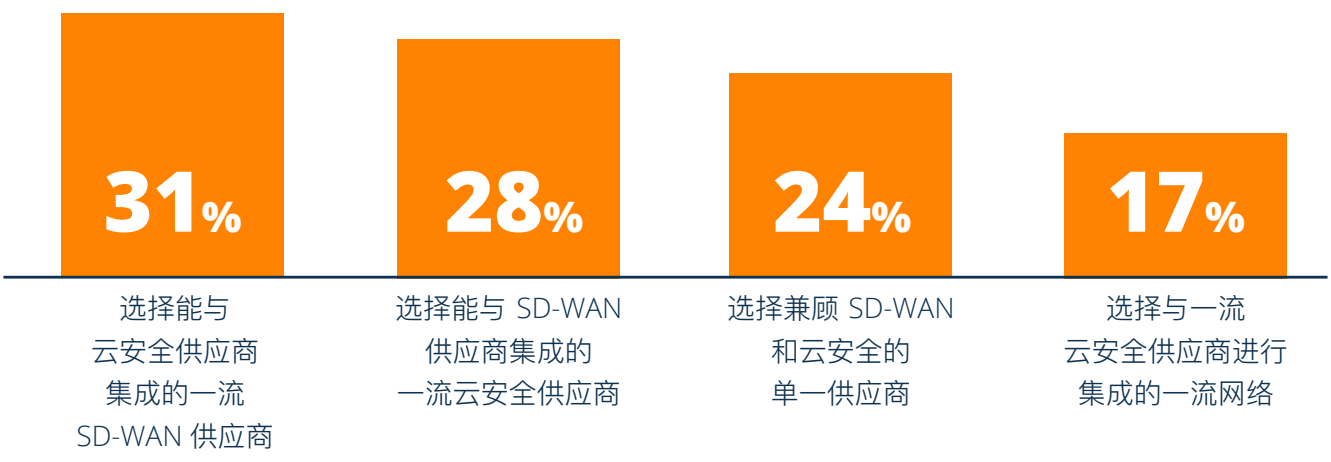
谁负责制定安全性架构决策？

多数组织是由网络团队主导安全决策工作，然后新的决策团队也开始出现：负责 IT 转型项目的个别项目团队。



是否正在考虑实施新的安全性架构？

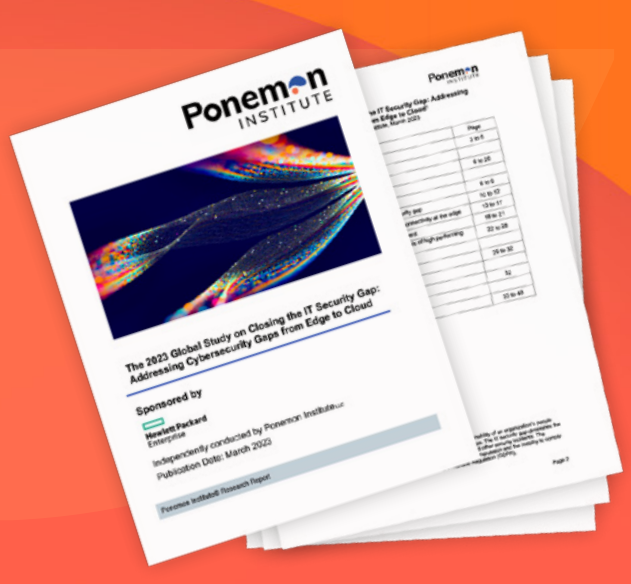
在部署 SASE 架构方面，一流 SD-WAN 和一流云安全服务的组合方案，以及单一供应商 SD-WAN 和云安全服务方案，几乎平分秋色，受到受访对象同等的青睐。



将高级的安全 SD-WAN 与一流 SSE（安全服务边缘）功能相结合，能够有效地将基于云的安全性服务融合到现有的网络和安全基础设施中，而选择单一供应商的优势则在于会让管理更简便。

阅读完整报告了解：

- 零信任与 **SASE** 解决方案的采用率和部署偏好
- 在弥合 **IT** 安全缺口方面，零信任与 **SASE** 发挥的作用
- 在弥合 **IT** 安全缺口方面，全面掌握组织网络情况的重要意义
- 与已落实有效网络安全和实施方案的组织相比，您的零信任与 **SASE** 架构实施进展如何



阅读报告 →

aruba
a Hewlett Packard Enterprise company