

# 2022 年 Thales 云安全研究

多云世界中数据保护面临的挑战

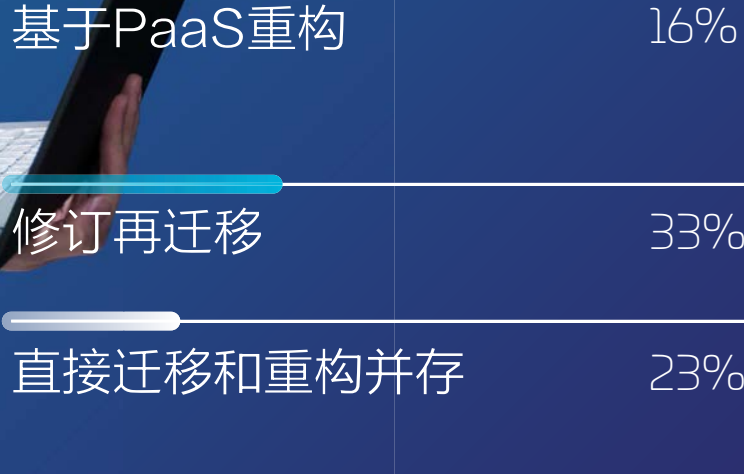
#2022CloudSecurityStudy

cpl.thalesgroup.com



## APAC 启用多云模式

APAC 企业将应用程序迁移到云的过程中，主要使用以下方式：



## 云的复杂性是一个主要问题



49% 的 APAC 受访企业认为，在云中管理隐私和数据保护法规比在内部部署网络中更复杂。



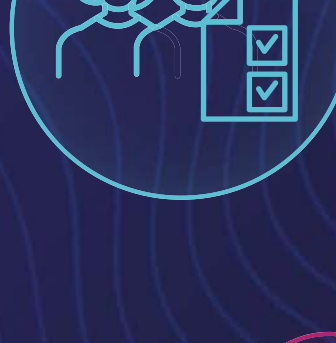
只有 19% 的 APAC 客户表示，他们有超过 60% 的敏感数据存储在外部云提供商处。

## 云安全策略和标准

当 APAC 企业被问及云安全策略、标准和执行时表示：



47% 的企业报告称，策略由安全团队集中制定，但技术标准的制定和实施取决于云交付团队。



38% 的企业报告称，策略和标准由安全团队使用其选择的工具集中制定和实施。



15% 的企业报告称，政策、标准和执行由云交付团队决定。

## 审核未通过和数据泄露

43% 的 APAC 受访企业报告称在某个时间点遭遇违约。

50% 的 APAC 企业报告称在某个时间点遭遇违约。

在过去的一年里，遭遇违约的 APAC 受访企业减少：2022 年的 32% 对比 2021 年的 39%。

## 云端加密

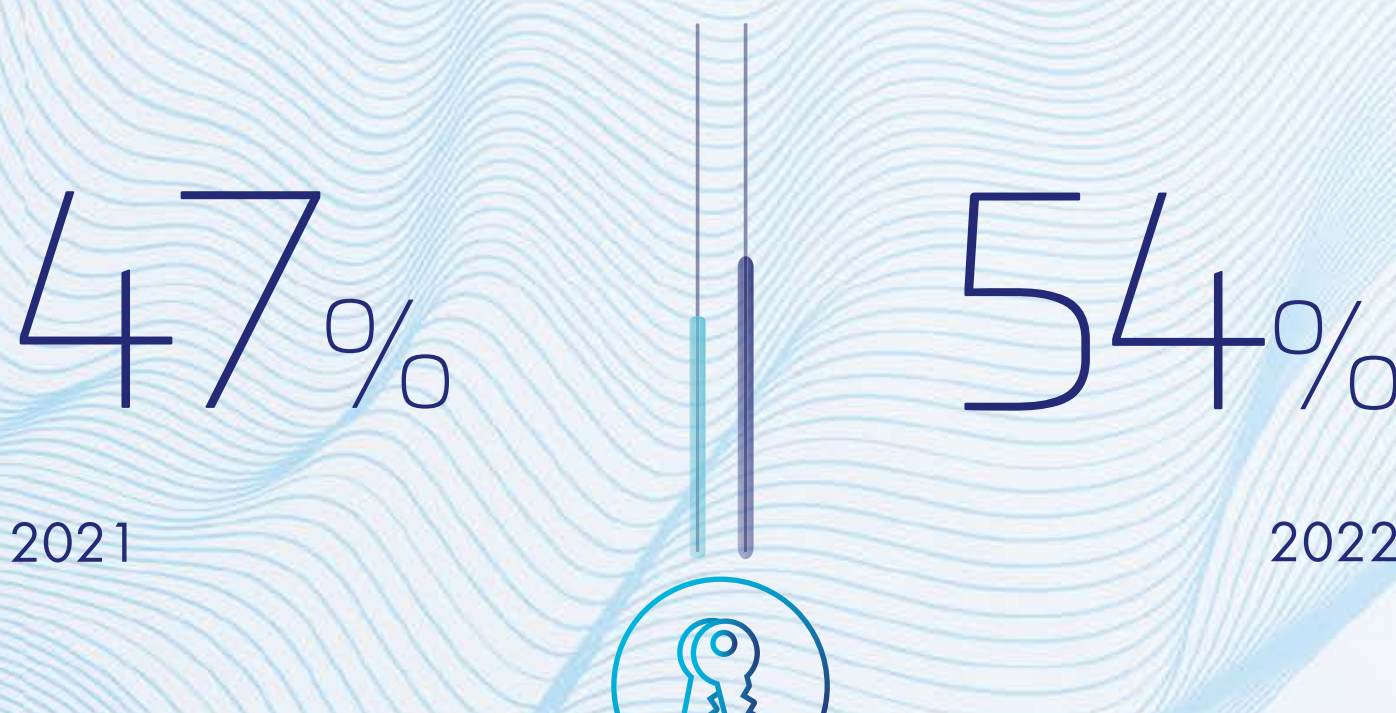
38% 得益于法规的“安全港”规定，30% 的 APAC 企业能够避免所需的违规记录程序。

46% 的 APAC 受访企业表示，内部安全架构决策是在云中何处以及如何使用加密的主要决定因素。38% 的 APAC 受访企业表示，监管合规是主要决定因素。

仅 21% 的 APAC 受访企业表示，其云中 60% 以上的敏感数据是加密的

## 加密密钥管理

今年在云控制台中管理密钥的 APAC 企业增加了 7%。



APAC 企业报告称，密钥管理扩展是一个问题。



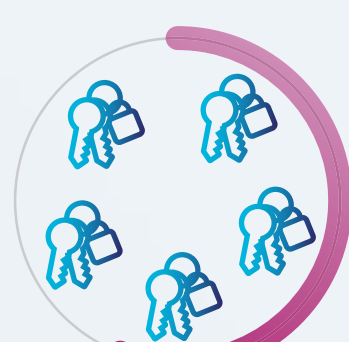
12%

的受访企业表示有 1-2 个密钥管理解决方案。



33%

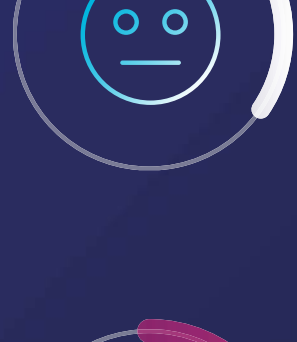
的受访企业表示有 3-4 个解决方案。



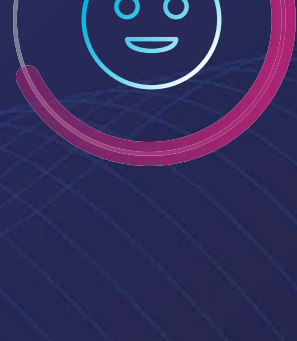
55%

的受访企业报告称有 5 个或更多的解决方案。

## 零信任



80% 接受调查的 APAC 企业表示，他们正在考虑、评估或执行零信任计划。



20% 的受访企业表示他们没有零信任的策略。



62% 的 APAC 受访企业表示，他们希望在云访问中利用零信任原则和技术。

访问 [www.safeplay.com](http://www.safeplay.com) 或加入公众号参加 11 月 17 日 (星期四, 下午 2 时至 3 时 15 分) 举办线上研讨会。听听 Thales 专家提供数据安全的建议。

