

2022 雲端安全研究年度報告

多雲世界中的資料防護挑戰

#2022CloudSecurityStudy

cpl.thalesgroup.com



亞太區走向多雲時代

亞太區企業將現有應用程式移轉到雲端的主要原因：



工作負載平移的組合	22%
為雲端和PaaS重新架構或重構應用程式	16%
回購和移轉	33%
工作負載平移與重新架構之間進行分工	23%

雲端複雜性是主要痛點



49%

的亞太區受訪者認為，在雲端中管理隱私和資料保護法規比在地端的網路中更複雜。



只有 19%

的亞太地區客戶表示，他們將超過 60% 的機敏資料存儲在外部雲端供應商那裡。

雲端安全策略和標準

當亞太地區端企業被問及雲端安全策略、標準和執行情況時：



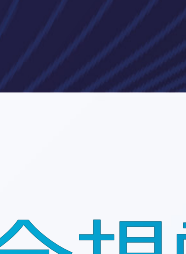
47%

的受訪者表示策略由安全團隊集中定義，但技術標準的定義和執行則由雲端交付團隊負責



38%

的受訪者表示，政策和標準是由安全團隊使用他們選擇的工具集中定義和執行的。



15%

的人表示，政策、標準和執行由雲端交付團隊負責。

違反合規需求和資料外洩

違反合規需求

43%

受訪的亞太區企業表示，曾在過去的某個期間沒有通過稽核。

資料外洩

50%

的亞太區企業表示，曾在過去的某個期間遭遇過資料外洩。

在過去的一年裡，亞太區的受訪者遭受資料外洩的比例有所下降：2022年為32%而2021年則為39%。

雲端加密

38%

的亞太區企業能夠避免必要的外洩通知流程，是由於法規中的“安全港”規定。

46%

的亞太區受訪者表示，內部安全架構的決策是雲端加密使用在何處以及如何使用的主要關鍵。38%的亞太區受訪者表示，監管合規性是主要驅動因素。

只有

21%

的亞太地區受訪者表示，他們在雲端中的機敏資料有60%以上是加密的。

加密金鑰管理

在雲端控制台管理金鑰的亞太區企業今年增長了7%。

47%

2021

54%

2022

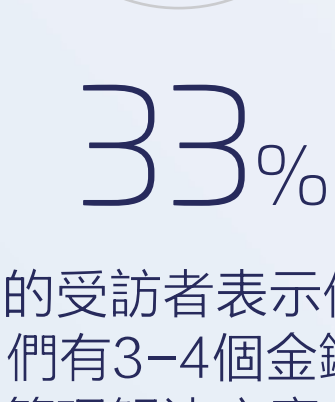


亞太區的企業在報告中指出，金鑰管理的擴張是一個問題。



12%

的受訪者表示他們擁有1-2個金鑰管理解決方案。



33%

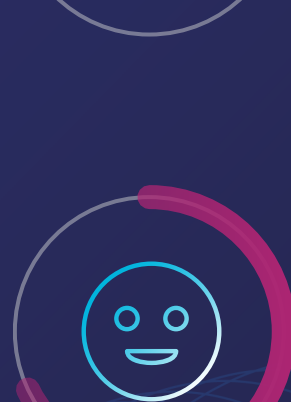
的受訪者表示他們有3-4個金鑰管理解決方案。



55%

的受訪者說他們有5個或更多的金鑰管理解決方案。

零信任



80%

受訪的亞太區企業表示，他們正在考慮、評估或執行零信任計劃。



20%

的受訪者表示他們沒有零信任策略。



62%

的亞太區受訪者表示，他們希望在雲端存取中利用零信任原則和技術。

請造訪 cpl.thalesgroup.com/apac-cloud-security-research 下載包括451 Research建議的完整報告。

451 Research
S&P Global
Market Intelligence

資料來源：由Thales委託S&P Global Market Intelligence 旗下 451 Research所進行2022 雲端安全調查