亞太版

THALES
Building a future we can all trust

2022 Thales 資料威脅報告

駕馭資料安全 – 在混合的工作環境、勒索軟體猖獗和加速雲端轉型的時代

#2022DataThreatReport

cpl.thalesgroup.com

無所不在的資料：我的資料在哪裡？

16%

2020研究顯示，只有16% 亞太區受訪者表示他們完全知道自己資料儲存位置。

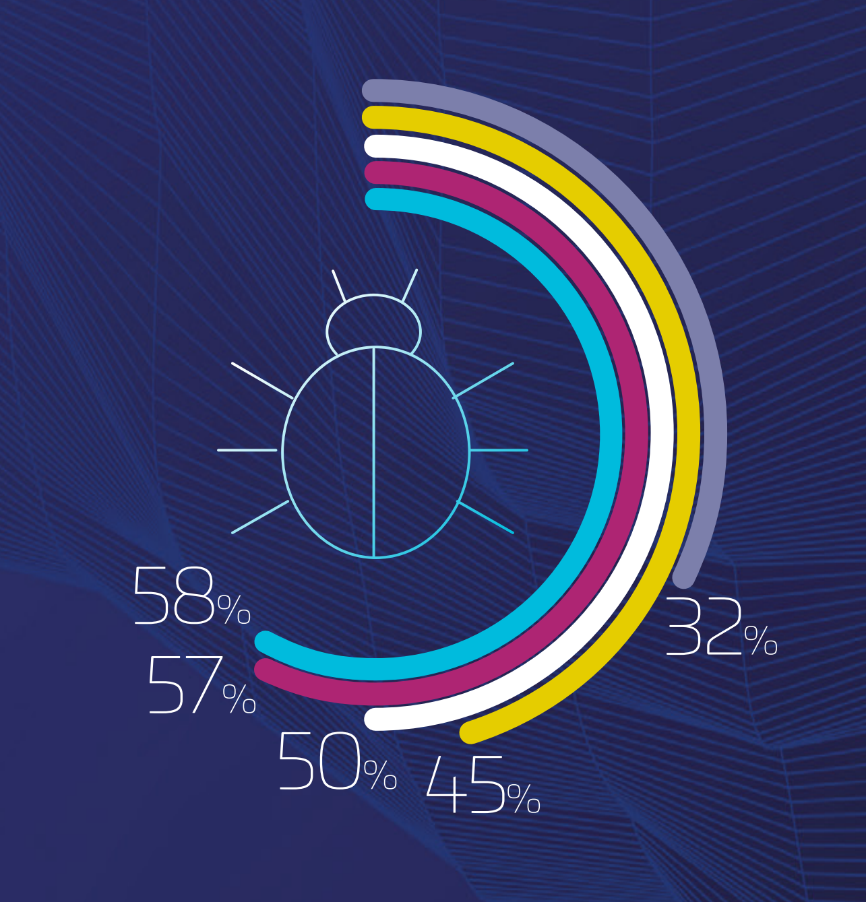
48%

的受訪者表示，他們至少有 40% 的機敏雲端資料已經加密。

21%

受訪者表示，他們至少有 60% 的機敏雲端資料已經加密。

資料外洩與安全的威脅，增加了管理的複雜性



- ● 將勒索軟體列為最主要增加的資安攻擊類型
- ● 將惡意軟體列為最主要增加的資安攻擊類型
- ● 將阻斷服務列為最主要增加的資安攻擊類型
- ● 過去經歷過資安漏洞
- ● 在過去 12 個月內發生過資料外洩

勒索軟體改變了資料外洩可牟取的非法利益

24%

的企業表示他們受到勒索軟體攻擊

27%

受到勒索軟體攻擊的企業造成營運的重大影響

only 47%

的受訪者已經遵循或將遵循正規的勒索軟體計劃

雲端動能

51%

受訪者表示他們至少有 40% 的資料儲存在雲端 ，19% 的受訪者表示將超過 60% 的資料儲存在雲端

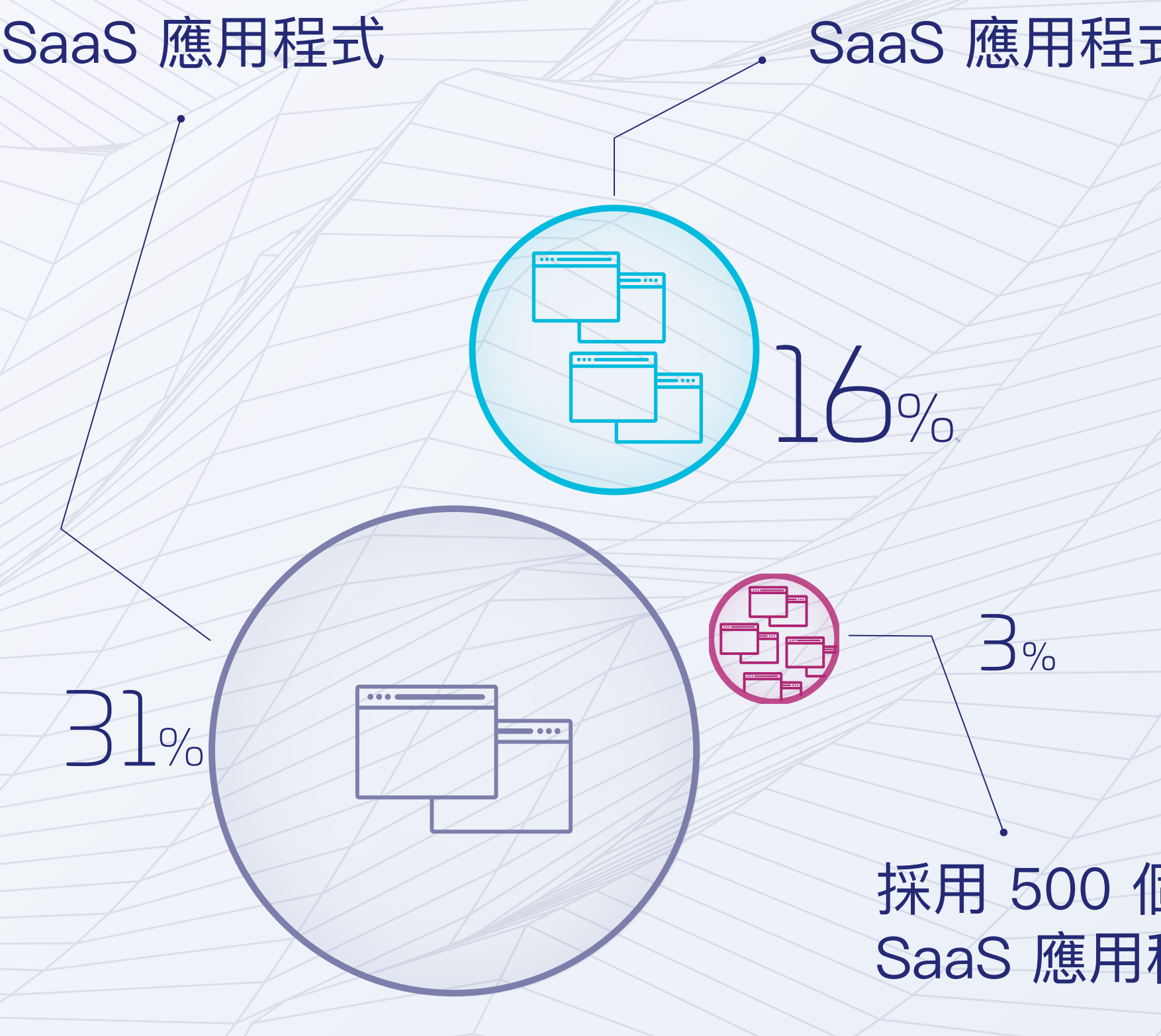
53%

的受訪者表示至少 40% 的外部儲存資料是機敏資料

26%

在報告中顯示，26%受訪者表示超過 60% 的雲端儲存資料屬於機敏資料

多雲環境



零信任策略

30%

的受訪者表示，零信任在 “很大” 程度上架構了他們的安全策略

48 %

的受訪者表示，他們採納零信任的 “部分概念”

量子運算

關於量子計算最受關注的三個問題

57%

網路加密風險

54%

現今資料的未來解密

52%

未來的加密危害

持續遠端辦公時代的安全風險和威脅

對安全的遠端存取解決方案充滿信心

24%

高度信心

34%

非常有信心

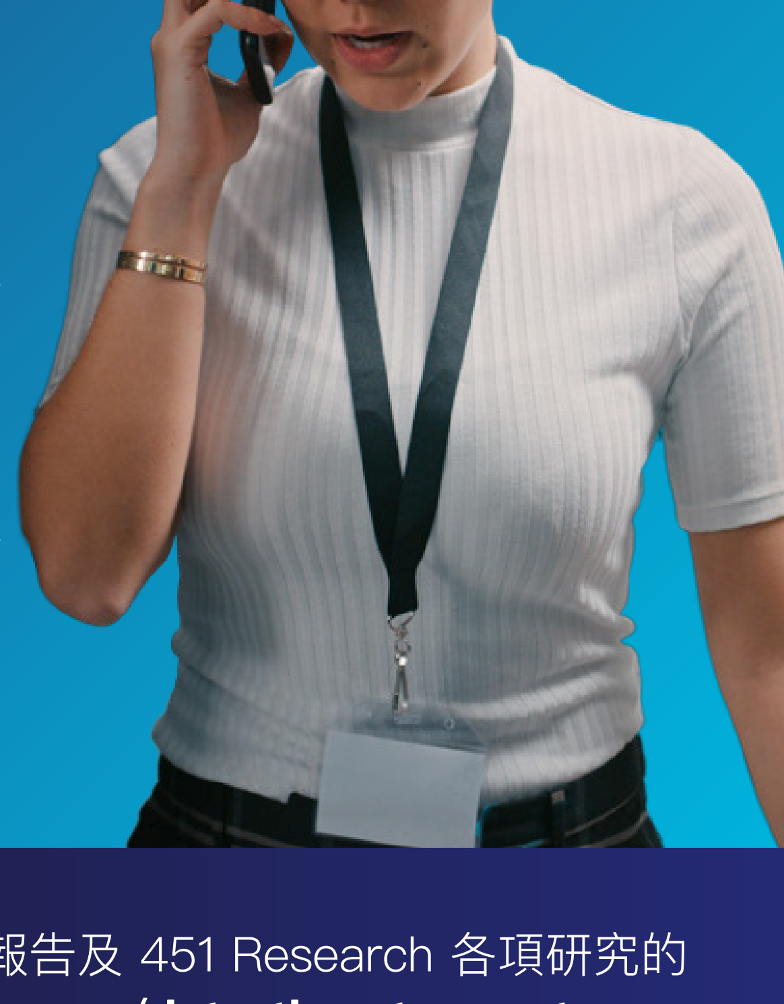
26%

有點信心

16%

完全沒有信心

零信任世界的資料安全



- 隨時隨地發現和分類資料
- 保護靜態、動態和使用中的機敏資料
- 在整個生命週期內控制用戶對機敏資料的存取和金鑰管理

下載 2022 Thales 資料威脅完整報告及 451 Research 各項研究的建議，請參閱 ： **cpl.thalesgroup.com/data-threat-report**

451 Research
S&P Global
Market Intelligence

Source: 2022 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales