亞太版

THALES
Building a future we can all trust

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

序言

2022 年 Thales 雲端安全研究年度報告是針對美國、加拿大、歐洲、亞太地區和拉丁美洲等 17 個國家/地區，近 2,800 名 IT 專業人員進行調查。 報告中部分有關亞太地區 (APAC) 關注重點資訊，是來自亞太地區澳洲、香港、印度、日本、新西蘭、新加坡和韓國七個主要市場的受訪者的回饋，其中包括 876 名中型到大型企業的受訪者。本研究探討整個受訪國家/地區的主要雲端和雲端安全趨勢。

在本報告中，我們除了探討亞太區的現行趨勢，我們也將今年度的研究結論，與全球/其他地區以及先前的研究相互比對，以及探究亞太區受那些關鍵因素的影響。 除非另有說明，本報告中的“受訪者”是指亞太地區的受訪者。

目錄

主要發現

- 大多數亞太區組織現在都採用了多雲方案，60% 的受訪者表示不止採用一個雲端服務供應商。客戶在其環境中使用廣泛且多樣的 SaaS、IaaS 和 PaaS 雲端解決方案。
- 日益增加的雲端複雜性是一個受到高度關切的問題，全球幾乎所有受訪者都對此表示贊同。
  - o 亞太區仍有大量工作負載和資料在雲端環境之外，比全球調查數據低了四個百分點。
- 雲端安全策略和標準是關鍵問題，正走向集中式雲端策略管控和執行的趨勢。
- 違反合規需求呈現上升趨勢，2021 年在於法規遵循上，違規的數量越來越多。
- 亞太區資料外洩率顯著低於全球平均水平，然而雲端資料外洩和違反合規需求的改善程度相對也較低。
- 加密技術很重要，特別是從監管角度來看更顯重要，無論是在地區或是全球範圍內，這些技術的採用率仍然偏低。
  - o 金鑰管理解決方案的擴張，是全球企業需面對的關鍵問題，它增加複雜性及額外的風險。
- 亞太區企業正在接受零信任，特別是在雲端環境中，儘管採用率的增長幅度不大。

“雲端複雜性的增加是一個主要需關切的問題，全球幾乎所有受訪者都對此表示贊同。”

43%

受訪者表示, 在過去的某個期間未通過稽核，與全球調查百分比相同。

55%

受訪者表示，使用 5 個或更多金鑰管理解決方案。

與世界上大部分地區一樣，企業指出了各種雲端採用的方法”

亞太區走向多雲時代

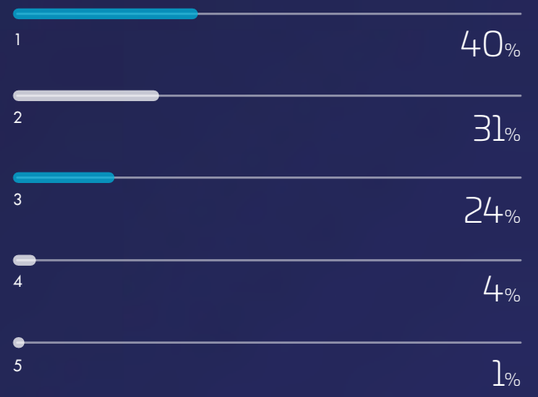
多雲的採用正在增加，60% 的受訪者表示採用多個雲端服務供應商《基礎設施即服務(infrastructure as a service; IaaS)、平台即服務(platform as a service; PaaS)、軟體即服務(software as a service; SaaS)》，比全球採用比率低 8%。 調查分析也顯示受訪者混合使用 SaaS、IaaS 和 PaaS 雲端平台的現況。

與全球大部分地區一樣，亞太區的企業回應各種採用雲端技術的方法。為什麼從現有應用程式遷移到 IaaS/PaaS 的原因，首要選擇是因為回購和移轉（33%），其次是為了工作負載平移(lift and shift) / 遷移現有應用程式 (22%)，和重新架構/重構應用程式 (16%)。與 2021 年的調查結果相似，也與其他國家地區結果一致。

圖表 1

多雲的增長

雲端IAAS服務供應商被使用於生產環境的數量



資料來源：451 Research 的 2022 雲端安全研究年度調查

受訪者表示他們混合使用 SaaS、IaaS 和 PaaS 雲端平台。”

雲端複雜性是主要痛點

雖然大量工作負載和資料分佈在多個雲端服務供應商之間，但仍有大量資料存放在雲端環境之外。”

多雲環境的多樣性導致了營運和安全的複雜性。近一半的受訪者認為，在多雲/混合雲端環境中，管理隱私和符合資料法規的遵循，比在本地端網路更複雜。雖然大量工作負載和資料分佈在多個雲端服務供應商之間，但大量資料仍然存在於雲端環境之外 。只有 19% 的受訪者將 60% 以上的資料儲存在外部雲端服務供應商，比全球平均低 了4 %。 這可能也顯示該地區對遷移到雲端仍猶豫不決。 大量的 SaaS 應用也導致了雲端運算的複雜性，16% 的受訪者表示超過 100個 SaaS的採用，31% 表示超過 50個 SaaS 的採用。”

只有

19%

受訪者將超過 60% 的機敏資料儲存在外部雲端服務供應商。

大量的 SaaS 應用也導致了雲端運算的複雜性 ”

雲端安全策略和標準

今年的調查發現，雲端安全政策與技術標準的確定和執行方式發生了轉變。近一半 (47%) 的受訪者表示，雲端安全策略由安全團隊集中定義，但技術標準和策略執行的定義則由各個雲端交付團隊負責，此項結果比 2021 年增加了 5%。超過三分之一 (38%) 受訪者表示，雲端安全政策、標準和執行均由安全團隊集中控管，15% 的受訪者表示這三者都由單獨的雲端交付團隊負責，比 2021 年減少 7%。日本在集中化控管的增加幅度最高 (14%)，而亞太區的平均增幅為 7% 、全球平均增幅為 2%；我們在其他亞太區國家也看到了相近的轉變。調查結果清楚地顯示，雲端政策的定義、控管和執行正在向集中化轉變，這可能是多雲部署在管理複雜度上要求越來越高有關，此結果與全球調查一致。

違反合規需求、資料外洩和雲端資料外洩

違反合規需求的稽查正在增加，43% 的受訪者表示，在過去的某個期間曾經有過違反合規需求。香港和印度受訪者在合規需求的違反率最高，分別是50% 和 49%，韓國受訪者的違反率最低（39%）。資料外洩率相較於 2021 年下降 7%，比全球平均低 11%，32% 的企業在過去一年表示有資料外洩事件發生，使亞太區企業是全球資料外洩最低的地區。 亞太區雲端資料外洩和未通過稽查的情況有所改善，33% 的亞太區受訪者在過去一年經歷儲存在雲端的資料和應用程式，發生資料外洩或違反法規遵循的事件，比 2021 年下降 4%，比全球他國家地區下降 2% 。 我們應該關注的是，法規遵循比率低可能是該地區合規制度不成熟和執法要求較低有關。

43%的受訪者表示在過去的某個期間曾違反合規需求。

雲端加密

加密技術是保護機敏資料免受網路攻擊所需的關鍵安全控制手段。受訪者提及靜態資料加密、代碼化和資料遮罩、傳輸中的資料加密以及金鑰管理/硬體安全模組是排名領先的保護技術。 重要的是，接受調查的亞太區企業中有 38% 表示，由於 “安全港 safe harbour” 監管規定，允許對加密或代碼化被盜取或外洩的資料做例外處理，他們避免了必要的違規通知。 亞太區與其他國家地區一樣，調查結果清楚顯示從這些技術中獲得的安全性和商業價值。 當被問及雲端中哪個位置要使用加密技術，以及如何使用的關鍵時，46% 的受訪者選擇內部安全架構的決策，其次是監管合規性，佔 38%，與全球平均相近。

對於隱私法規高度重視與約束的國家/地區的受訪者，通常將合規性列為最重要的推動因素。 加密對於保護雲端環境至關重要，但雲端機敏資料的加密仍然難以實現，只有 21% 的受訪者表示，雲端中 60% 以上的機敏資料已經加密，接近全球平均。 這也凸顯了企業需要提高這些關鍵保護措施的採用和成熟度，以防止資料外洩與違反合規性。

只有

21%

的受訪者表示，雲端中 60% 以上的機敏資料已經加密，接近全球平均。

38%

亞太區企業受訪者表示，由於 “安全港 safe harbour” 監管規定，允許對加密或代碼化被盜取或外洩的資料做例外處理，他們避免了必要的違規通知。

加密金鑰管理

金鑰管理是全球企業面臨的共同挑戰，金鑰管理擴張尤其令人擔憂。只有 12% 的受訪者採用 1– 2 個金鑰管理解決方案，而 55% 的受訪者使用了 5 個或更多，與全球結果相近。這說明了儘管有解決方案可以降低複雜性、降低風險、提高安全效率和可靠性以及降低成本，但問題依然存在。在混合的加密金鑰管理策略上，受訪者在雲端控制台執行金鑰管理的比率增加 7%，這顯示企業已開始將金鑰管理解決方案整合到集中式平台。這降低整體複雜性和保護雲端環境的複雜性，特別是對於需要使用跨環境標準化工具的多雲企業。

零信任

亞太區企業正在採用零信任策略，對於管控上有最大效益的機敏資訊和功能的存取，開啟零信任之旅。 超過四分之三 (80%) 的企業表示他們正在考慮、評估或部署零信任計劃，雖然 2022 年的增長幅度不大，但仍顯示零信任趨勢仍在延續，也反映企業的積極跡象。更多採用零信任的雲端存取是另一個關鍵趨勢。 受訪者被問及他們希望在哪裡使用零信任原則和技術，62% 的受訪者提到了雲端存取，與全球結果相同。

當被問及零信任對他們在雲端安全戰略制訂時，有多大程度的影響，30% 的人表示非常大的影響，48% 的人表示使用了一些零信任概念，22% 的受訪者表示零信任不會影響雲端安全戰略，與全球百分比一致。總體而言，調查資料顯示，零信任對亞太區受訪者的重要性逐年略有增加。

80%

的企業表示他們正在考慮、評估或部署零信任計劃

22%

受訪者表示零信任不會影響雲端安全戰略，與全球百分比一致。

結論

調查資料顯示，雲端的複雜性不斷增加。超過 60% 的亞太區受訪者，使用一個或以上的雲端服務供應商，並且業務應用程式持續並快速向雲端遷移。 雲端複雜性是一個主要問題，多雲環境的數量增加了營運和安全挑戰。 近一半的受訪者表示，雲端環境中的隱私和資料保護更為複雜，原因之一可能是仍有大量資料儲存在雲端之外，這也是企業對移轉機敏資料仍有疑慮且放緩採用雲端的一個關鍵指標。在接受調查的大多數亞太區國家/地區受訪者，採用集中式雲端安全策略定義、執行的趨勢正在增加，85% 的受訪者表示採用集中式策略定義，遠高於全球的比率。

2022 年違反合規的稽查有所增加，與全球趨勢一致。 2022 年的資料外洩數量有所減少，比全球平均低11%，使亞太成為全球資料外洩率最低的地區之一。 亞太區在 2022 年雲端發生資料外洩或違反法規遵循的事件，比 2021 年下降 4% 。

雲端資料加密對於整體資料安全和避免違規通知至關重要，38% 受訪者，由於加密或代碼化的資料，避免了違規通知。作為雲端加密需求的關鍵推動因素，內部安全架構的排名高於合規性的要求，這是一個積極的指標，顯示企業從根本就將加密直接建構到雲端建置的項目中，而不是由於監管要求被迫採用。雖然在雲端資料加密方面有很大的進步，但仍只有五分之一的受訪者表示他們的大部分機敏雲端資料已經加密；在這方面顯然有很多工作需要推動。金鑰管理仍然是企業面臨的挑戰，金鑰管理的“擴張”是一個主要問題：超過一半的企業表示，使用了五個金鑰管理解決方案。幸運的是，許多企業已經開始在雲端平台集中管理金鑰，這對於多雲環境來說更是關鍵。

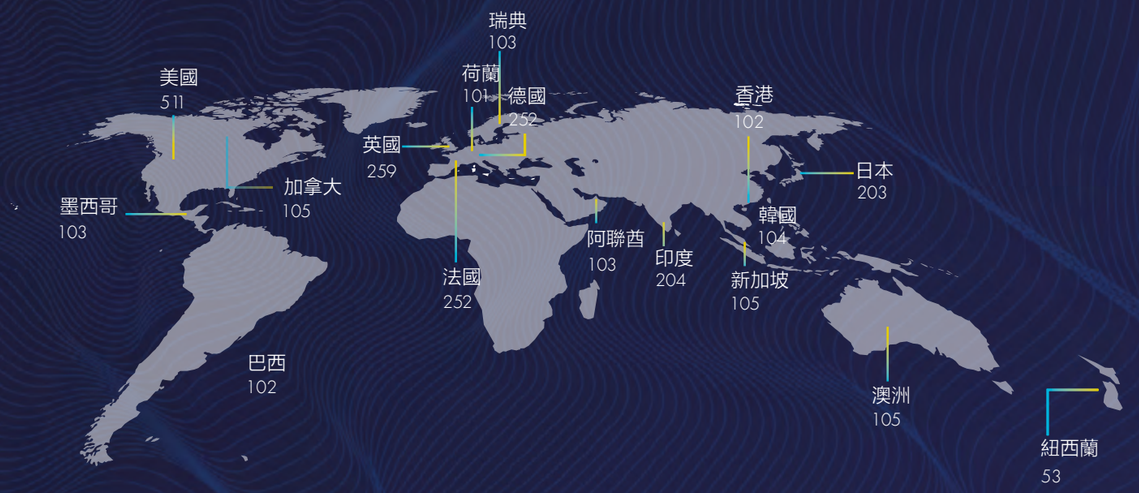
零信任作為一種核心安全方法持續獲得企業的認可，重點是敏感資料和功能的存取，尤其是在雲端應用程式和資料中。大多數亞太區受訪者表示，他們至少有一個基本的零信任策略計劃，隨著越來越多的企業意識到在雲端和本地端部署零信任概念的價值，這一趨勢將會持續下去。

關於這項研究

隨著企業要超越過去兩年疫情早成迫切行動的影響，他們正在努力保護現今營運更複雜的環境。

2022 年Thales 雲端安全研究報告全球版，針對全球安全專業人員和領導階層主管進行了廣泛調查，探討當今資安環境的各個方面，議題遍及加速數位化轉型、雲端移轉，和在多雲環境中複雜的安全管理等問題。 2022 年Thales 雲端安全研究報告匯集近 2,800名安全專業人員和高階管理者的調查資料，其中包括來自亞太地區 876 名受訪者。

這項研究是作為一項觀察性研究進行的，沒有任何因果關係。



產業領域

製造業	157	消費品	107
零售	154	計算機/電子/軟體	106
科技	127	工程	104
金融服務	120	聯邦政府	103
醫療保健	115		
公共部門	109		

營收

1 億美元至 2.499 億美元	162
2.5 億美元至 4.999 億美元	802
5 億美元至 7.499 億美元	865
7.5 億美元至 9.999 億美元	458
10 億至 14.9 億美元	254
15 億美元至 19.9 億美元	58
20 億美元或更多	168

Source: 451 Research's 2022 Cloud Security custom survey

THALES
Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/apac-cloud-security-research