THALES
Building a future we can all trust

亞太版

2023 Thales 資料威脅報告

數位主權和轉型的願景與步驟

#2023DataThreatReport
cpl.thalesgroup.com

關鍵發現

在這份報告中，我們分享了全球資料威脅報告 (DTR)研究中，以亞太區為重點的調查結果，並簡要討論了數位主權的機遇和挑戰以及未來需要關注的要點。 事實上，亞太區的許多 DTR 調查結果與全球分析數據非常接近，我們也分析出一些關鍵性的差異。

62%

人為疏失比駭客入侵更危險：

雲端資料外洩的第一大主因是“人為錯誤”。

企業在調查中表示，正在使用授權讓他們的用戶避免錯誤。 亞太區採用強多因子身份認證的比例已上升至 62%，比去年增加了 6 個百分點，32% 的受訪者認為，身份和存取管理是保護機敏資料免受網路攻擊最有效的安全技術，這顯示亞太區愈來愈重視防範人為錯誤的發生。

無論雲端的成熟度如何，多雲已經是事實。

超過四分之三 (80%) 的亞太區受訪企業，在一個以上的公有雲中執行各項工作，每個企業平均使用 2.3 個雲端服務供應商，這與全球調查相同。

雖然內部對安全的關注度正在提高，但安全成果仍然落後。

超過四分之三 (80%) 的亞太區受訪者，仍然相信他們企業的系統會保護他們的個人資料，略低於全球百分比。

然而 34% 的人表示，他們在過去 12 個月內發生過資料外洩事件。

數位主權是一項新興的策略措施。

96% 的受訪者認為，指定或更改資料的位置/管轄權或全方面資料加密，是實現各種不同程度數位主權的可行方案。

58% 的亞太區企業，擁有超過五個以上的企業金鑰管理系統，略低於全球百分比 (62%)，此舉會增加管理的複雜度。

雲端風險意識正在趕上採用雲端服務。

76%

的亞太區受訪者對 5G 有安全顧慮，其中大多數受訪者表示最大的憂慮，是保護連接到 5G 網路的人和設備的身份，這與全球的調查結果相似。

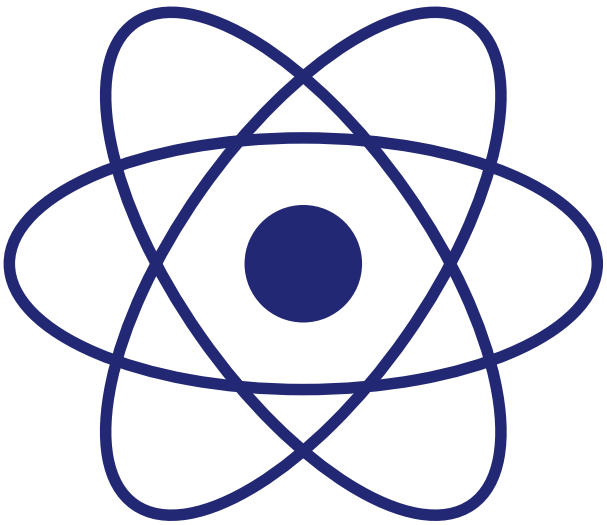
全球受訪者調查指出，網路攻擊的第一和第二目標，分別是以 SaaS 模式的雲端交付（38%）和以雲端為基礎的儲存（36%）； 亞太區受訪者的結果與全球相同，只是百分別略有不同（分別為43%和37%）。

在打擊勒索軟體議題上，結果喜憂參半。

50%

23%

50% 的亞太區企業製定了正式的防制勒索軟體計劃，在 Thales 2022 年首次調查此議題時比例為 47%。 近四分之一 (23%) 的亞太區受訪者表示他們曾遭受過勒索軟體攻擊，這一比率略高於全球平均水準，比 2022 年略有下降。值得關注的是，儘管攻擊數量顯著下降，在亞太區和全球調查受訪者回應，受到勒索軟體攻擊造成重大影響的企業略有增加 。



後量子密碼學進一步從學術研究走向現實世界。

60%

的亞太區受訪者表示，網路破密是最值得關注的量子運算安全威脅。

法規的不斷改變和外部攻擊事件，需要資料安全的快速回應能力。

82%

的亞太地區受訪者非常或有點擔心，資料主權與隱私法規會影響企業的雲端部署計劃。超過一半 (58%) 的人認為在雲端環境中管理隱私和資料法規遵循，比企業內部網路更複雜，略高於全球比率。

期待數位主權

企業的核心關注點是數位主權。 數位主權使企業對產品和服務中使用的資料、硬體和軟體，能夠更自由地運用。 它使企業能夠更好在本地端執行隱私權控管，以維護機敏和可公開身份資料的安全資料管理，進而遵守全球跨境的各種隱私、資料安全和彈性法規。 數位主權是企業優化他們的系統和架構的一個重要機會，同時為股東和公民提供更好的服務。

超過四分之三 (82%) 的亞太區受訪者，對於資料主權與隱私法規會影響雲端部署計劃的進行，有點或非常擔心。

調查中問到：企業需要了解並簡化多雲資料安全策略。 82% 的亞太區受訪者表示，他們有些或非常擔心，這與全球比例 (83%) 相似。 96% 的受訪者認為，指定或更改資料的位置/管轄權或全面資料加密，是實現雲端/數位主權等不同要求的可行方案。

82%

的亞太區受訪者，對資料主權與隱私法規會影響雲端部署計劃的進行，有點或非常擔心。

57%

的亞太區受訪者，使用雲端服務供應商的金鑰管理器或加密金鑰，導致他們完全依賴供應商，進而無法決定本身企業的資料主權。

超過一半 (57%) 的亞太區受訪者，使用雲端服務供應商的金鑰管理器或加密金鑰，導致他們完全依賴供應商，無法控制自己的資料主權。

企業需要簡化且靈活地運用各種加密方案，以滿足不同的營運和資料主權要求。 超過一半 (57%) 的受訪企業，已將全部或大部分加密金鑰控制權，委託給雲端服務供應商，略低於 2022 年的 59%。

54%

簡單化是關鍵。 超過一半 (54%) 的亞太區受訪者擁有 5–10 個金鑰管理器，這也增加跨多雲時統一管理資料的複雜性和成本。比 2022 年增加了 9%。

回歸本質

與消費者、合作夥伴、客戶和監管機構等利害關係人協同合作，可以更好地保護資料安全。 資料安全計劃能夠用非正規的方式制定，因此需要新的協作模式。 透過讓所有利害關係人都能保護資料，企業可以為日益動態的市場提供更強大、更靈活的控制基準。

簡單化是關鍵。 超過一半 (54%) 的亞太區受訪者擁有 5–10 個金鑰管理器，這也增加跨多雲時統一管理資料的複雜性和成本。比 2022 年增加了 9%。這可能是由於愈來愈多的多雲組織， 超過一半的亞太區企業選擇使用雲服務供應商提供的金鑰管理器。

數位主權對企業來說是短期，也是長期的機會。 雖然資料法規不斷變化，企業需要更即時的回應與遵循法規，但來自任何單一雲端服務供應商的長期資料、營運和軟體獨立性，驅使企業採用新雲端技術，以實現戰略增長目標。 企業獨立採用任何單一雲端服務供應商，可以維持更多資料安全控制，並可靠地將控制措施應用在最具執行價值的環境。

關於本調查研究

這份全球性的調查報告，是針對全球 2,889 名受訪者，在 2022 年 11 月至 12 月間，透過網路對每個國家/地區的目標對象進行線上問卷調查，目標對象是安全和 IT 管理專業人士。 除了一般知識性的調查主題外，年收入企業的篩選標準是需高於 1 億美元的企業（部分特定國家受訪企業需界定為 1 億美元至 250 美元之間 ）。 這項研究是作為一項觀察性研究進行的，沒有提出因果關係。 從全球研究分析的數據做為報告基準，亞太區版本主要調查七個主要市場，包括澳洲、香港、印度、日本、紐西蘭、新加坡和韓國的 888 名受訪者。

S&P Global
Market Intelligence

調查來源：2023 資料威脅報告由 Thales 委託 S&P Global Market Intelligence 執行。

贊助單位

EXCLUSIVE NETWORKS

THALES
Building a future we can all trust

全球辦公室與聯絡資訊
請參閱
cpl.thalesgroup.com/contact-us.

cpl.thalesgroup.com/data-threat-report