CPL.thalesgroup.com #2020DataThreat

THALES

報告摘要
2020 Thales資料威脅報告

亞太版

簡介

今日企業面對因為市場與供應鏈中斷而帶來的前所未有挑戰。企業必須重新檢視、重新評價，某些情形下還必須重新創造基本營運方法。現在的成功取決於是否採納數位轉型技術，包括雲端、行動、人工智慧、機器學習與物聯網(IoT)。數位轉型扮演關鍵角色，協助企業適應今日持續演進的商業條件，以及做好準備迎接「後疫情」商業事實。六月間的2020 IDC COVID Tech Index Survey調查報告顯示，資安、IoT與5G技術的採購增加，而其他傳統IT支出指數則下滑，這些結果印證了上述趨勢的形成。

> 45%受訪者認為他們在安全方面將超過原定的2020年預算。

目前，亞太區在數位轉型方面落後其他地區。不過這似乎意謂著亞太企業有機會藉由加速轉型而超越其他國家。事實上，IDC調查顯示亞太某些公司已在進行數位轉型。我們調查的亞太企業超過四分之一(26%)正積極顛覆他們參與的市場或者嵌入數位能力以提升企業敏捷性。

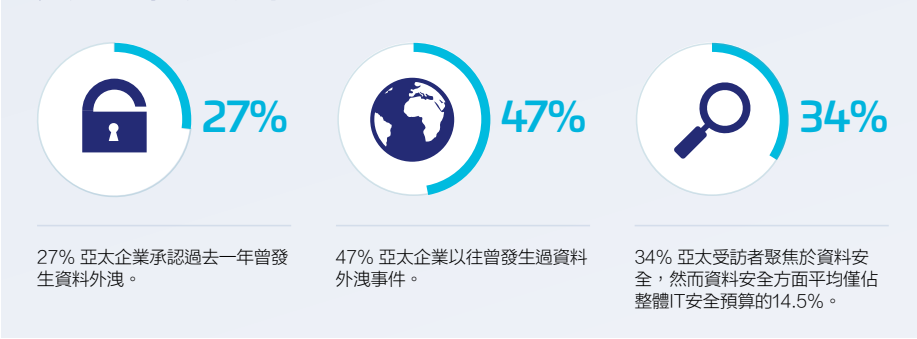
數位轉型可以提供極大價值，但也使得資安變得更複雜，而因為疫情而轉向在家工作的結果也加大此一複雜性。加速數位轉型有助於解決今天的挑戰，但安全團隊必須跟上商業／IT團隊，因為他們可能產生更多安全弱點，同時也要因應疫情增加的資安事件。隨著更多員工從遠端工作，公司將更加仰賴儲存在雲端的大量資料。所有這些因素都使得今日資料環境的安全維護變得更複雜，而亞太的一些資安障礙例如資源、人員、程序與預算等也增添了此一複雜性。

然而，亞太企業在資安方面似乎存在認知不一致的問題。52%相信他們非常或極為安全，但他們並沒有針對升高的資料風險建置適當保護所需的程序和技術。超過半數發生過資料外洩或者沒通過安全稽核。雲端資料安全維護方面，大多數公司欠缺正確的觀念，錯誤的尋求雲端服務供應商承擔公司本身應負的資安責任。

疫情因素使得安全比以往更加重要。IDC的COVID-19 Impact on IT Spending Survey (調查期間2020年6月4-15日)顯示，45%受訪者認為他們在安全方面將超過原定的2020年預算，20%表示安全預算不會改變。顯然，在家工作模式已對安全支出產生實質影響。所有受訪國當中，安全預算將超過原定2020年計畫的受訪者比例以澳洲和中國最高，分別為50%和47%。比例最低的是紐西蘭和印度。

疫情非僅影響安全產品，同時也包括安全建置人員。當IDC問到「第一波經濟復甦到來時，貴公司最需要建立／重建／聘雇的IT技術為何？」，亞太受訪者最多人回答的是「網路安全」。所有受訪國當中，最強調網路安全重要性的是澳洲和印尼。

資料威脅無所不在



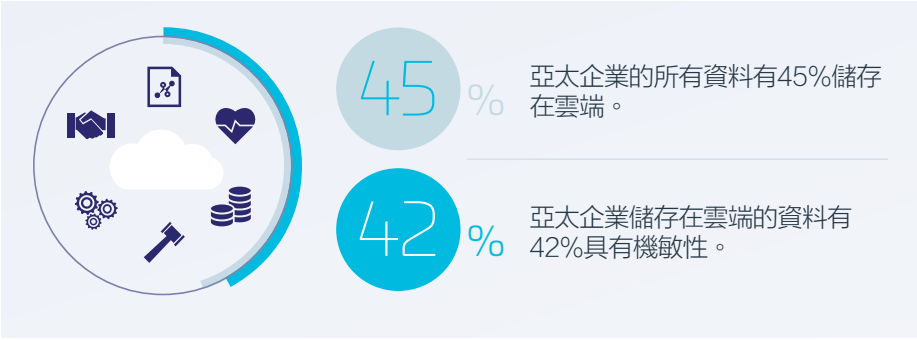
> 27%亞太企業承認過去一年曾發生資料外洩，47%亞太企業以往曾發生過資料外洩事件。

圖一：資料威脅無所不在

資料來源: 2020 Thales 資料威脅報告調查, IDC, 2019 年 11月

不幸的是，沒有任何企業可以免除資料安全威脅，尤其疫情開始之後的全球資料外洩事件已增加。即使是在疫情之前，27%亞太企業承認過去一年曾發生資料外洩，47%亞太企業以往曾發生過資料外洩事件。再者，這些企業在網路安全方面的支出仍不成比例，僅34%亞太受訪者聚焦於資料安全，然而資料安全方面平均僅佔整體IT安全預算的14.5% (全球資料安全的平均支出略高，佔整體IT安全預算的15.7%)。

雲端機敏資料成長中



> 45%資料儲存在雲端，其中42%具有機敏性。

圖二：雲端機敏資料成長中

資料來源: 2020 Thales 資料威脅報告調查, IDC, 2019 年 11月

所有受訪亞太企業都將一些機敏資料儲存在雲端。我們的調查顯示，企業儲存在雲端的資料接近反折點，他們表示約有45%資料儲存在雲端，低於全球樣本的50%。更重要的是，亞太受訪者表示雲端資料約有42%具有機敏性。

雲端是否建置足夠安全性？

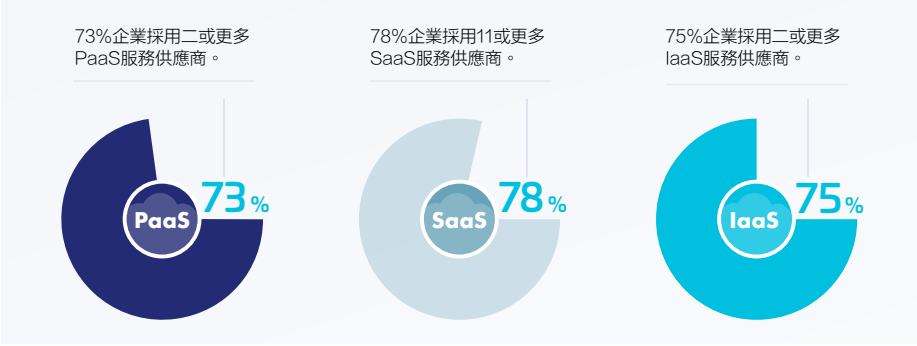
> 儲存在雲端的機敏資料只有52%採加密保護。

圖三：雲端是否建置足夠安全性？

資料來源: 2020 Thales 資料威脅報告調查, IDC, 2019 年 11月

隨著更多機敏資料儲存到雲端，資料安全風險也跟著提高。然而，儘管有著如此顯著的機敏資料暴露，但資料加密與代碼化的比例還是很低。事實上，99%亞太受訪者至少有一些儲存在雲端的機敏資料沒有加密。儲存在雲端的機敏資料只有52%採加密保護。

是的，這是一個多重雲世界



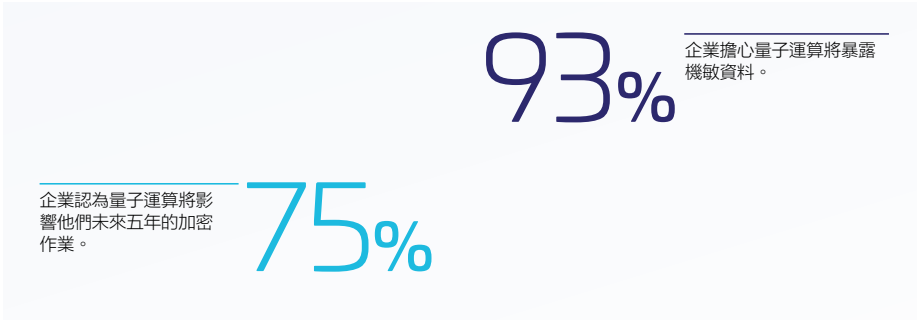
> 78%亞太企業採用11或更多SaaS服務供應商

圖四：是的，這是一個多重雲世界

資料來源: 2020 Thales 資料威脅報告調查, IDC, 2019 年 11月

更多資料轉移到雲端之後，安全問題變得更複雜。不過此種複雜性通常是自己造成的，因為多重雲越來越普遍使得IT管理人員的注意分散到許多方向，而且往往導致多重未整合的加密金鑰管理系統。73%亞太企業採用二或更多PaaS服務供應商，78%企業採用11或更多SaaS服務供應商，而75%企業採用二或更多IaaS服務供應商。

為量子運算做好準備？



> 93%亞太企業擔心量子運算將暴露機敏資料。

圖五：為量子運算做好準備？
資料來源: 2020 Thales 資料威脅報告調查, IDC, 2019 年 11月

在新興威脅方面，量子運算將使得資料安全變得更加複雜。一旦量子運算上線時，加密需求將產生基本上的改變，75%亞太企業認為量子運算將影響他們未來五年的加密作業，93%企業擔心量子運算將暴露機敏資料。

零信任世界的現代化資料安全

圖六：零信任世界的現代化資料安全
資料來源: 2020 Thales 資料威脅報告調查, IDC, 2019 年 11月

企業面對不斷擴大且更複雜的資料安全挑戰，他們需要更聰明、更好的方法維護資料安全。亞太企業需要採取零信任模式及多階層的資安維護，以擁抱雲端安全。運用存取管理技術對存取應用程式、網路的使用者與裝置進行驗證與認證，同時也要部署更強韌的資料發現、強化、資料外洩預防以及加密方案。重要的是，企業採用靈活架構以實現信任模組，資料安全不應破壞企業在追求數位化轉型所做的努力。

IDC指南

- 資料安全方案尤其是加密，對於警覺 COVID-19 疫情之後的資料風險管理至關重要。尤其現在的居家工作模式，迫使有些採用自有裝置工作的員工，必須存取和修改更大量的企業資料。
- 企業需要新的資料安全方法以保護「後疫情」IT環境，因為資料已從地端轉移到雲端，然後又回到地端，而且無法確定員工是否將選擇回到辦公室。
- 明確的了解資料安全與網路安全對於企業營運與商業結果的關聯性。
- 數位平台非僅在面對網路威脅上需要具備彈性，而當事件真的發生時也應具有敏捷的因應能力。
- 投資現代化、混合與多重雲資料安全工具以實現責任分擔模式。
- 考慮採用一種安全的最低特權模式，以確保資料和使用者存取安全。
- 加強資料發現方案與集中化金鑰管理以強化資料安全。
- 藉由強韌的分類以補強資料發現，強化資料法規遵循能力。
- 針對量子運算對加密產生的衝擊效應做好準備。
- 聚焦於正確的威脅向量。
- 強化SaaS商業應用程式的資料安全能力。

關於本報告

本報告的調查對象是以全球總樣本1,723筆中的500多位負責或影響IT與資料安全的亞太經理人為主，包括澳洲、印度、印尼、日本、馬來西亞、紐西蘭、新加坡和韓國。報告由Thales委託IDC執行調查、報告與分析。

下載完整報告：
cpl.thalesgroup.com/APAC-DTR

關於Thales

那些保護您隱私的組織仰賴Thales保護他們的資料。企業在維護資料安全上面對越來越多重要的決策，不論是建置加密策略、轉移到雲端、或者資料法規的遵循義務等，您可以仰賴Thales以確保安全的進行數位轉型。

關鍵時刻的關鍵技術。

感謝我們的贊助者

THALES

聯絡我們

辦公室地點與聯絡資訊請參觀
cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

cpl.thalesgroup.com/apac-data-threat-report

#2020DataThreat