FUJIFILM
Value from Innovation

減輕 IT、資料及列印安全攻擊的威脅

企業如何增強資安韌性

轉型邁向成長茁壯：企業的數位轉型

在《從生存到繁榮：運用企業韌性實現競爭優勢》一文中，我們展示企業如何在快速變化的環境中維持韌性，讓企業組織更加強大並蓬勃發展。採用明確、高效率工作流程和勞動力配置的公司在危機中展現更強大的韌性。

全球企業可以預期，2023 至 2027 年間，以下趨勢將推動組織轉型。

提早擁抱數位轉型的企業相比慢速前進的企業，成長速度快 5 倍。[1]

現在，關鍵在於敏捷

包括大型以及中小型企業 (SMB) 在內的韌性及策略性企業皆展現能力，以數位轉型賦能其混合及遠端團隊，確保企業成功並增強社會責任。

FUJIFILM
Value from Innovation

許多企業正在努力追趕，部分企業表現優於其他企業。現今環境讓後發者有機會在技術採用及創新文化方面，彌補與業界領導者的落差。後發者運用早期採用者的學習，加快數位化及成長的速度。

在打造韌性及健全的組織文化心態中，長期數位轉型意味著塑造串聯的工作空間、育成混合及遠端團隊的協作、透過工作流程自動化達成想像中的未來工作，以及增強勞動力的技能，為創新做好準備。

探索本系列精彩內容：

1

未來的勞動力: 簡化工作流程，團隊生產力更智慧

2

減輕 IT、資料及列印安全性攻擊的威脅：企業如何增強 IT 安全性韌性

3

改造工作空間，在數位時代成長茁壯：改造工作空間的趨勢及策略

企業轉型邁向成長茁壯，藉由數位轉型提升速度及生產力。

相較於採用創新速度最慢的公司，超過期望的公司實現快 4 倍[2] 的成長。此成長率甚至比早期採用的公司更高，證明無須犧牲獲利能力，就能實現企業數位轉型。

目錄

05
資安：APAC 企業日益擔憂的問題

08
APAC 企業的最大資安挑戰

19
打造 IT 策略的檢查表

22
與台灣富士軟片資訊共同成長茁壯

26
參考資料

07
深入了解 APAC 資安威脅環境

13
保護企業免於 IT 威脅

21
IT 網路防護是企業的最優先事項

24
與台灣富士軟片資訊共同踏上轉型旅程

資安：
APAC 企業日益擔憂的問題

增強資安 — 與保護電腦、網路及資料等的企業資產並防止未授權存取的網路安全策略有關 — 是亞太地區 (APAC) 企業的最大新擔憂。

網路威脅正在快速進化，網路攻擊造成的後果也日趨嚴重。除了金錢上的損失外，企業的實際成本包括資料損失、形象受損和業務中斷。

這些趨勢突顯 APAC 企業加強資訊安全能力的急迫需求

企業需要有效的資安策略。但是，打造策略不是終點，而是一段旅程。人們通常會將資訊安全視為需要大規模解決方案，但即使是細微的改變，也有助於增強公司的安全態勢。

在本指南中，我們將深入探討 APAC 的安全威脅環境，並將重點放在企業面臨的最大資訊安全挑戰上，旨在協助公司找出現有策略不足之處，讓公司得以採行必要的解決方案，改進資訊安全防護。

亞太地區面對全球最高的網路攻擊次數，占全球網路安全事件的 31%。[3]

2023 年第 1 季，APAC 每週網路攻擊次數出現最高的年增幅（1,835 次攻擊／週）。

此數字比全球平均（1,248 次攻擊／週）高 47%。[4]

深入了解 APAC 安全威脅環境

部署後門程式是網路攻擊者的首選，其次是勒索軟體及 MalDocs。[5]

馬來西亞及菲律賓企業遭受亞太地區最多的安全事件。[6]

澳洲企業最不可能訂定事件回應計畫，香港則最有可能。[7]

新加坡企業主要擔憂業務中斷。[8]

企業因應資訊安全事件所採行的五大措施[9]

68% 進行定期訓練或沙盤推演

64% 採行事件回應教戰手冊、計畫或政策

62% 訂定遭入侵後的復原計畫

62% 指派資料保護長

62% 延聘網路安全專家

APAC 企業的最大資訊安全挑戰

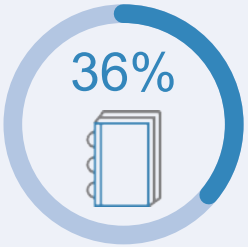
了解資安挑戰能讓企業防範營運中斷、收益損失和資料遭竊

公司應投資在全方位組織策略，以涵蓋資安的各個層面。

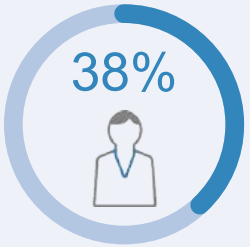
深入了解關鍵挑戰，找出並彌補資安流程中的漏洞。

克服業務與資安間的優先性不一致

CIO 與企業主管的業務目標不一致時，可能難以實施資安措施，甚至導致投資不足。



的 APAC 企業在 2022 年沒有任何事件回應教戰手冊、計畫或政策。



未指派資料安全長，或是長期諮詢網路安全專家。[10]

不確定自身資安防護足以抵抗網路攻擊者的新策略。[11]

FUJIFILM
Value from Innovation

員工的資料保護教育

人為錯誤是雲端資料洩漏的首要原因。[12] 有許多因素會造成人為錯誤，主要是機會、環境和缺乏意識。[13]

人為錯誤引發資料洩漏的範例包括下載病毒感染軟體、密碼強度不足、IP位置遭入侵。

造成人為錯誤的因素：

機會

接觸的次數越多，犯錯的可能性就越高。

環境

工作空間的實體環境和辦公室文化會對人為錯誤有所影響。在某些情況下，員工雖然知道該採取的正確行動，但卻沒有這麼做。

缺乏意識

使用者可能單純不知道該採取何正確行動。

因應資安人才短缺

2022 年，全球網路安全工作者的短缺加劇 26.2%，達到 342 萬人。[14]

APAC 面臨前所未見的人才短缺，網路安全工作者的缺口高達 216 萬人。[15]

造成此種短缺的因素包括缺乏進修資安的進階課程、[16] 對安全產業的誤解，以及技術的快速演進。[17]

人才短缺也突顯需找出更完善的方法，以保護機密資料及數位資產的重要性。

因應雲端的資安挑戰

隨著公司轉往雲端以滿足 IT 需求，APAC 的雲端導入程度快速成長。

但是，轉換為雲端運算是複雜的過程，必須從一開始就納入資安考量。如果未針對雲端移轉採行有效策略，即容易產生資料洩漏、資料損失及雲端設定錯誤的風險。

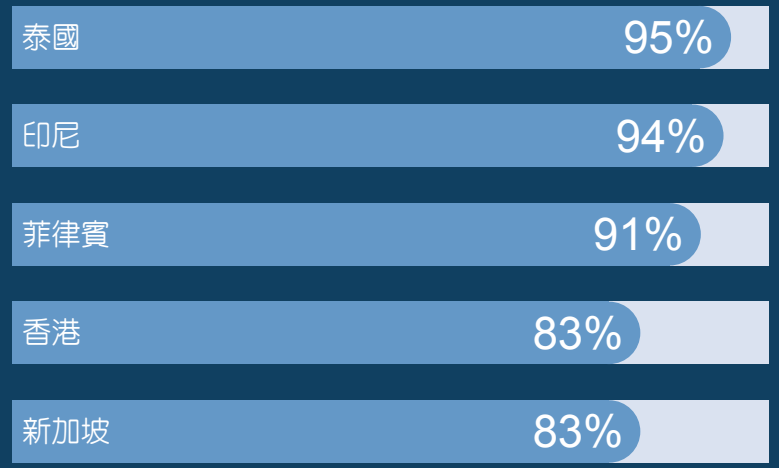
APAC 雲端導入程度近況

APAC 企業的雲端相關支出將在 2024 年前達 2,000 億美元。[18]

已採用雲端服務的企業仍預期增加雲端投資。

在亞洲，每五家企業就有四家 (84%) 規劃在 2024 年前進行完整的雲端移轉。

雲端投資的增加最有可能來自[19]：



防範網路解密的準備

隨著企業將資料及運算轉往雲端，安全性團隊必須使用加密傳輸守護企業的數位足跡。

但是，網路攻擊者會解開加密的訊息、密碼和金鑰，導致機密資訊外洩並危及系統。量子運算雖仍在開發中，但若落入有心人士手中，將會對公司造成極度威脅。

2023 年，APAC 公司所面臨的最大網路安全挑戰之一是網路解密的量子運算安全威脅。

大約 60% 的 APAC 企業將網路解密視為量子運算安全威脅的最大問題。[20]

數位空間的防護

連網裝置的數量會持續成長，因此，企業發現保護裝置免受威脅越來越困難。這是因為：

1. 現代勞動力擁有有史以來最多的連網裝置，員工通常會使用多種連網裝置執行日常的工作，包括桌上型電腦、筆記型電腦、智慧型手機、平板電腦及多功能事務機s。

2. 連網裝置收集和傳輸的資料量大幅增加，進而讓網路攻擊者獲得更廣泛的攻擊範圍。

3. 大多數連網裝置在設計時未考量資安，用來防範網路攻擊的資安控管措施不足，例如，定期更新軟體，或是製造商或廠商提供的安全修補。

行動安全威脅：

- 網路釣魚攻擊、惡意應用程式、易受攻擊的網路、中間人 (MiTM) 攻擊[21]

列印安全威脅：

- 內部威脅：其他使用者在未授權的情況下操作、意外犯錯造成資料洩漏
- 外部威脅：軟體竄改、裝置儲存的文件資料洩漏、稽核記錄竄改、竊聽及竄改通訊資料、對管理功能的未授權存取

保護企業免於 IT 威脅

企業必須研擬強大的安全計畫應對確知的資安挑戰。

下面列出企業防範安全威脅的建議。

挑戰	建議
克服業務與資安間的優先性不一致	在組織內建立網路韌性
員工的資料保護教育	在工作空間宣揚網路意識
因應資安人才短缺	
因應採行雲端的安全挑戰	延聘外部 IT 專家服務，以輔助 IT 部門
做好防範網路解密的準備	
數位空間的防護	為裝置訂定資安計畫

在組織內建立網路韌性

網路韌性是指組織預測、反應以及從網路攻擊復原的能力。

有鑒於網路攻擊日趨精密，您必須優先建立網路韌性。在過去，駭進系統需要一天以上的時間，但是，現代的惡意活動只需數個小時就能完成。訂定現代化的整合式資安計畫和系統，讓企業能迅速地抵禦攻擊至為關鍵。[22]

建立網路韌性的要素[23]

1

預測

了解組織的資產、弱點及潛在威脅。

2

承受

採行系統、流程及工具，以保護資料和連網裝置的安全。

3

復原

及時復原十分重要，務必確保已訂定事件回應計畫，將資安事件的影響降到最低。

4

進化

從過去的事件學習，然後實施您獲得的洞見，以彌補組織資安措施中的可能漏洞。

在工作空間宣揚網路意識

即使採用尖端技術，員工經常成為企業資安中最弱的一環。

推行網路意識訓練課程有助於解決此問題。這類課程能讓團隊學到關於最新資安威脅、最佳實務，以及業界專門法規及法規遵循規定的知識。

此方法能將發生資安事件的風險降到最低，並提升對相關業界法規的遵循性，因為這兩者皆有助於提升資安防護。

工作空間網路意識最佳實務

在組織內全面進行網路意識訓練。

根據主管和員工的需求客製化訓練內容。

避免僅此一次的方法。

定期進行訓練，讓團隊了解最新威脅和攻擊技巧。

安排網路釣魚模擬及測試。

找出資安策略中的弱點部位，協助員工在模擬中找出及避免網路釣魚。

延聘外部 IT 專家服務，以輔助 IT 部門

考量大多數企業安全團隊無法處理的新挑戰，例如，應對大規模網路解密或確保雲端移轉順利，讓 IT 團隊獲得值得信賴且具備能力的 IT 專家服務支援，保證讓您領先網路攻擊者不只一步。

舉例而言，為了對抗網路解密，IT 專家可以協助公司：

- 確認機密資料是否會輕易地遭解密
- 持續更新加密技術

在雲端移轉時，IT 專家會監控並指導公司完成移轉過程，確保公司採行符合法規的正確程序、事件回應計畫，以及定期進行演習和模擬。

企業可以運用外部 IT 專家服務消除潛在的問題和漏洞。IT 專家將頻繁進行評估並及時升級，讓您能持續遵循法規，並在發生問題時主動處理，而非被動以對。

APAC 公司與代管、專業資安服務業者合作的原因[24]：

- APAC 內的資料洩漏事件增加
- 數位轉型導致雲端部署增加
- 克服資安專家的短缺
- 對外部安全專業知識和法規遵循見解的需求成長
- 減少內部雇用安全專家的支出，以及有效進行安全管理

為裝置訂定安全性計畫

企業必須採行能夠跨端點提供防護的資安解決方案，涵蓋桌上型電腦、筆記型電腦、平板電腦、伺服器、智慧型手機及其他連網裝置。

此外，列印裝置必須具備因應網路攻擊的防護。列印是各企業常見且頻繁進行的活動，因此，大量的企業資訊皆經由印表機處理。

要打造安全列印策略，您必須：

- 確保所有與企業網路連線的裝置獲得安全保障。。
- 確保企業內的所有連網裝置皆遵循相同的安全標準及政策。
- 使用提供機密列印放行功能的解決方案，保護印表機輸出的安全。
- 採用提供最新防護能力的代管列印服務，以應對日益精密的網路威脅。此方法最適合經常依賴列印並採用分散式列印環境的企業。

印表機安全性：需實施的關鍵功能

機密列印放行

安全列印放行可將列印工作保留在安全的虛擬佇列中，直到收到最終列印命令為止，且使用者需親自前往印表機。員工必須透過 PIN 碼、ID 卡、行動應用程式或掃描 QR 碼等各種方式完成身分驗證，才能放行列印工作。

此功能幫助您將常見的印表機使用錯誤降到最少，例如，未拿取列印工作、機密列印文件放在印表機無人處理，或是有人不慎拿取屬於別人的機密文件等情況。

安全行動列印

安全行動列印可讓員工使用連網裝置安全地提交工作，且通常內含驗證、加密、使用者驗證、記錄及稽核等功能。

安全行動列印對於特定工作環境十分關鍵，例如，企業已實施混合工作配置，且員工必須在異地工作並從自己的裝置列印時。

對於醫療及金融業的企業而言，這也是不可或缺的功能，因為這類公司必須遵循文件安全的法規規範。

360° 資料安全

360° 資料安全內有各種能確實提供防護的措施，包括安全掃描、阻止未授權存取、稽核軌跡和即時裝置監控。

重要功能包括單鍵使用者驗證（讓您可以有效地管理使用者及列印環境）、增強稽核能力，以及透過安全網路進行端對端資料加密。

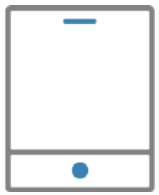
打造 IT 策略的檢查表

下面列出打造 IT 策略的建議：

評估組織的資安能力

- ☐ 評估各團隊成員的技能和專業知識。
- ☐ 評估資安團隊的資源配置。評估預算是否符合組織的安全需求。
- ☐ 製作計畫，以應對改進事項和團隊內的技能缺口。
- ☐ 深入了解有助於增強組織能力的解決方案，例如，延聘外部 IT 專家服務。

實施打造網路韌性的計畫



- ☐ 進行評估，以確認組織的資產、弱點及潛在威脅。
- ☐ 列出保護資料和連網裝置安全所需的系統、流程及工具。
- ☐ 建立完善的事件回應計畫。透過沙盤推演和模擬，定期測試及更新計畫。
- ☐ 監控資安基礎設施。定期檢視及更新策略。

實施網路意識訓練課程

- ☐ 確認網路意識訓練課程的目標。
- ☐ 準備訓練課程的內容。
- ☐ 安排員工訓練課程，確保訓練教材及課程能讓所有人輕易地了解。
- ☐ 監控、評估訓練課程的成效。
- ☐ 定期更新內容及訓練教材，確保課程跟上威脅環境的最新演進。

實施連網裝置的計畫

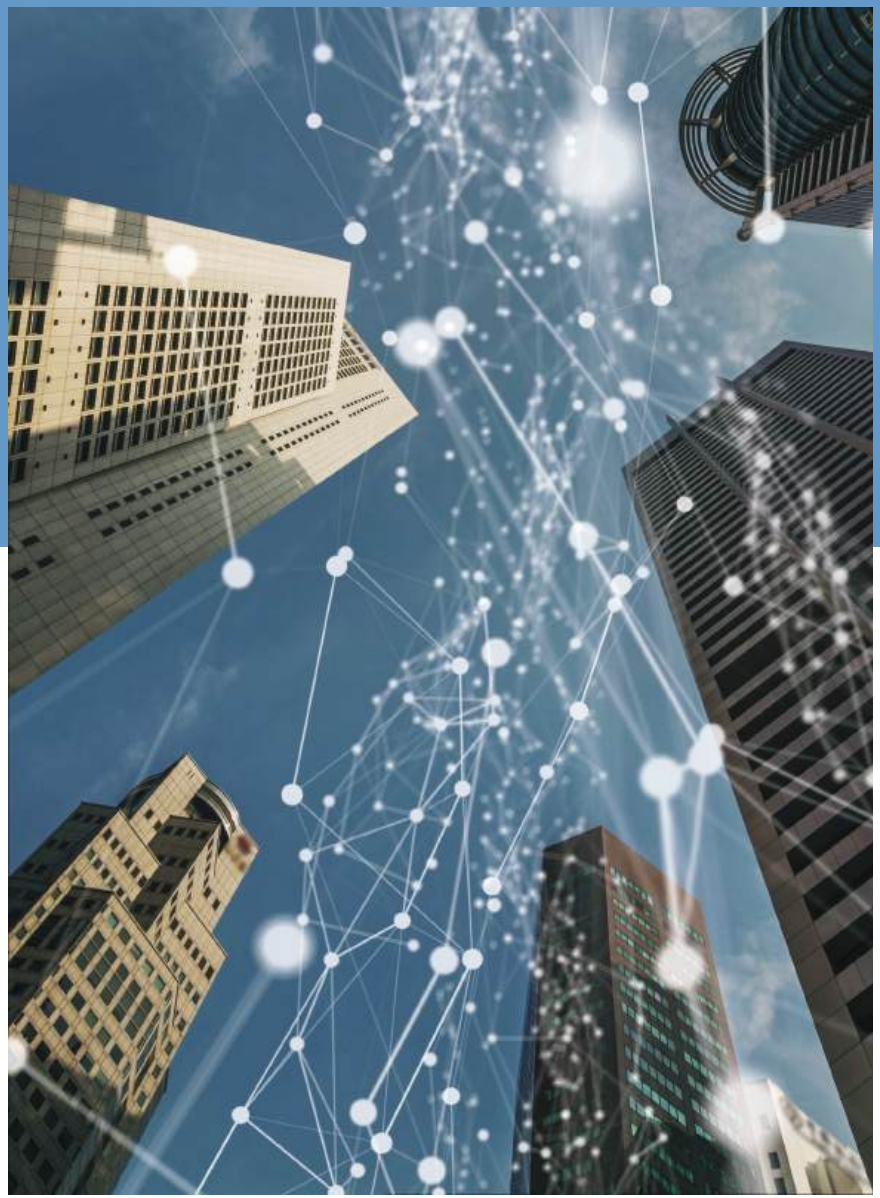
- ☐ 盤點組織內印表機及連網裝置。
- ☐ 針對列印及連網裝置實施使用者驗證，確保只有獲得授權的人可以存取裝置。
- ☐ 確認所有印表機及連網裝置皆使用最新版本的軟體。
- ☐ 檢視每一裝置的安全功能。採用具有重要列印安全功能的解決方案，例如，機密列印放行和安全行動列印。
- ☐ 採用提供最新防護能力的代管列印服務，以應對列印安全威脅。
- ☐ 確認組織的網路意識訓練課程涵蓋印表機及連網裝置防護的相關資訊。

IT 網路防護是企業的最優先事項

由於全球安全攻擊在 APAC 不斷升高，亞太地區的企業必須把資安放在第一位。在威脅日趨嚴重的情況下，保護網路、資料以及包括印表機在內的裝置安全是企業逐漸注重的問題。

為了有效應對不斷改變的威脅環境，您必須跟上最新的資安趨勢及挑戰，並訂定可用來實施可靠安全解決方案的靈活計畫。此策略方法可讓您透過後續流程及強大的 IT 合作關係，以增強安全。

台灣富士軟片資訊是值得您信賴、可靠且專業的資安合作夥伴，為您的 IT 團隊提供正確的解決方案和支援。



與台灣富士軟片資訊共同成長茁壯

Fujifilm 的全系列數位技術及自動化解決方案能協助您進行數位轉型。

ApeosWare Management Suite 2 是一款有助於進行全方位裝置管理、整合式驗證、機密列印輸出、記錄總計、文件分配及追蹤資訊外洩的列印管理軟體，它簡化文件管理，為企業提供無法估量的價值。

IT Expert Services 是一款針對中小型企業量身打造的全方位代管 IT 支援服務。採用 IT Expert Services 時，SME（中小型企業）能獲得高技能的 IT 專業人員協助，讓他們能將心力專注在推動業務上。

MPS（代管列印服務）Guardia 是一款 FUJIFILM Business Innovation 推出的新世代代管列印服務，能保護企業免於成本超支、資料洩漏及生產力損失。

Ysoft 是一款專注處理文件擷取和 3D 列印管理的列印管理軟體。此模組化列印管理軟體可靈活擴充，讓企業能依照需求的成長迅速地擴充和部署其他功能。

PaperCut 是一款印表機、影印機和多功能事務機 (MFD) 內建的列印軟體，能用來監控及管理組織的列印輸出、協助使用者將浪費降到最低，並獲得簡易安全的列印經驗。

與台灣富士軟片資訊共同踏上轉型旅程

有了我們的解決方案及專業知識，企業界將邁出通往長遠轉型的下一步。探索貴賓客戶與我們合作的心得。

我們透過客戶調查獲得寶貴的洞見：

96%

的客戶認為與我們開展業務十分順暢

98%

的客戶認為我們是能夠滿足所有需求的理想創新夥伴

97%

的客戶很樂意推薦採用我們以滿足所有商業需求

FUJIFILM
Value from Innovation

讓我們協助您增強資訊安全

隨著網路威脅在規模和精密度方面增長，企業必須把資安放在第一位。台灣富士軟片資訊能為您提供可靠的解決方案，協助您防護公司的網路。

我們以客戶為本，為合作夥伴打造出色的經驗是我們引以為豪之處。我們與客戶保持緊密聯絡，因此能為您實施量身打造的正確解決方案。

台灣富士軟片資訊隨時為您效勞，協助您在快速改變的 IT 安全性環境中找出一條前進的路。我們也會協助您釋放數位轉型的完整潛力，確保您的企業可對抗安全威脅。

做好準備，迎向未來

聯絡台灣富士軟片資訊

FUJIFILM
Value from Innovation

參考

1.2. Accenture, Scaling Enterprise Digital Transformation, August 2021

3. IBM, IBM Security X-Force Threat Intelligence Index 2023, March 2023

4. Check Point Research, Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most, April 2023

5,6,7. Kroll, State of Incident Response: APAC, October 2022

8. IBM, IBM Security X-Force Threat Intelligence Index 2023, March 2023

9.10. Kroll, State of Incident Response: APAC, October 2022

11. EY, Global Information Security Survey, July 2021

12. Thales, 2023 Thales Global Data Threat Report, June 2023

13. Usecure, The Role of Human Error in Successful Cyber Security Breaches, June 2022

14.15. ISC2, Revealing New Opportunities for the Cybersecurity Workforce, October 2022.

16. Deloitte, Finding cybersecurity talent in an altered world, February 2023

17. Advantis Global, The Cybersecurity Talent Shortage: Understanding the Urgency and Impact, July 2023

18. Boston Consulting Group and Cisco, The Future of Cloud in Asia Pacific, August 2021

19. Alibaba Cloud, A Majority of Asia Businesses Expect to Increase Cloud Investment in 2023, March 2023

20. Thales, 2023 Thales Global Data Threat Report, June 2023

21. Tech Target, Top 4 mobile security threats and challenges for businesses, May 2021

22. CNBC, Palo Alto Networks CEO warns companies need modern, integrated cybersecurity: ‘The bad actors are moving faster’, August 2023

23. IDC, Leadership in a Changing Digital World: Five Mandates, April 2023

24. Frost & Sullivan, Asia-Pacific (APAC) Managed and Professional Security Services Market: The Shortage of Cybersecurity Professionals is Driving MSS and PSS’ Future Growth Potential, November 2022