Microsoft Security

資料安全性索引

趨勢、洞察力和策略，確保您的資料安全性，
並指引生成式 AI 旅程

2024 年報告

前言

隨著我們對不斷演進的資料安全性環境展開第二年的研究，擺在我們面前的挑戰和機遇從未如此深刻。在過去的一年中，資料安全性事件的嚴重性有增無減。在這個以資料為中心的時代，用來保護資料的策略和工具也在快速演進。

今年，我們將探討一個新領域：生成式 AI 對資料安全性策略的作用和影響。

AI 正以前所未有的能力在全球掀起浪潮，釋放更多創新與效率。然而，儘管擁有如此巨大的潛力，組織也關注資料安全性風險以及如何塑造資料安全性團隊的責任。我們認為 AI 能加速組織強化其基礎資料安全性實務，讓他們能做好準備，將資料過度分享和資料洩漏的影響降至最低，並建立安全性採用 AI 的流程。另一方面，AI 也能協助組織強化資料安全性實務，包括找出隱藏的風險與防護缺口、建議防護政策以及協助更快速地調查與修正安全性事件。

我們的研究目標是為資料安全性領導者提供可行的見解與指導，協助其團隊有信心地調整資料安全性策略，有效保護 AI 的使用，並將 AI 整合至其資料安全性策略中。雖然 AI 的影響範圍與潛力相當驚人，但它只是席捲企業的最新轉型浪潮，例如混合式辦公、雲端與行動化，近年來，此問題突顯出在使用過程中對可視性的永恆需求，以降低風險並發揮最大影響力。根據這些經驗，妥善保護 AI 所使用的資料以及使用 AI 來強化資料安全性措施，將可提高生產力、韌性和靈活性，讓團隊在面對未來的挑戰時更得心應手。

我們邀請您探索最新的研究結果，並希望這些洞察力能協助您強化資料安全性態勢以及激勵您擁抱 AI 並建立全面的資料安全性策略，釋放更多創新，並確保我們所有人都能擁有更安全的未來。

Rudra Mitra
公司副總裁
Microsoft 資料安全性與合規

引言

企業每年平均會發生 156 起資料安全性事件，這些事件的影響仍是資料安全性決策者持續關注的問題。這是有充分理由的：單一事件可能會造成巨大的財務和商譽損害，尤其是在威脅不斷演變的環境中，攻擊者會利用任何可能的漏洞。如果沒有足夠的保護和安全性措施，使用者可能會意外或惡意地將敏感的關鍵業務資料（包括員工和客戶資訊、智慧型財產、財務預測和營運資料）置於風險之中。當組織尋找新的方法來保護這些範圍廣泛的敏感資料時，許多決策者已將注意力轉向急速崛起的 AI。

AI 的挑戰並不單一。鑒於三分之二的組織承認其員工正在使用未經授權的 AI 工具，因此確保員工安全性使用 AI 工具至關重要。與此同時，也有機會在精密的資料安全性策略中，將 AI 運用為有效的工具。

AI 驅動的資料安全性解決方案已經在即時識別和應對威脅、改善資料安全性計畫的整體速度和準確性以及提供有助於在資料安全性事件發生之前加以預防的洞察力等方面發揮了關鍵作用。組織必須管理 AI 所帶來的風險，此外還要利用其力量來識別人類以機器速度處理和分析時可能面臨挑戰的模式，並最終擊退日益複雜的網路攻擊。

Microsoft 在 2023 年委託獨立研究機構 Hypothesis 對 800 多位資料安全性專業人士進行跨國調查，並開始進行資料安全性指數計畫，更好地服務我們的合作夥伴和客戶，並協助企業領導者制定自己的資料安全性策略。

在 2024 年，本報告在先前研究的基礎上，針對超過 1,300 位資料安全性專業人士進行擴大的多國調查，並提出新的見解。儘管資料顯示我們所調查市場的一致見解和趨勢，但我們也發現了全球最新的資料安全性和 AI 實務與趨勢的新知識。

重要發現

1

資料安全性景況仍然分崩離析，因此更需要具凝聚力的資料安全性策略，應對傳統與 AI 使用相關的新風險。

各組織對其資料安全性措施的滿意度和信心都很高。然而，資料安全性事件的嚴重性卻持續上升，特別是因為組織發現其目前的資料安全性政策與 AI 應用程式的使用 / 導入增加之間存在差距。面對這些利害關係和當務之急，許多組織仍然依賴多種資料安全性工具，這可能會增加他們的整體弱點和風險。

2

隨著終端使用者越來越多採用 AI 應用程式，組織最敏感資料的完整性面臨更大的風險，需要更多的可視性和新的保護控制措施

隨著 AI 工具成為日常工作中不可或缺的工具，組織也開始關注資料安全性風險。他們意識到有必要加強防禦，並致力於防止 AI 造成的資料安全性事件 - 但這些工具的未授權使用突顯了更強大的可視性需求。

3

決策者對於 AI 提升資料安全性的潛力感到樂觀

各組織正積極投資於結合 AI 的資料安全性工具，改善偵測與回應能力。AI 可協助偵測未受保護的資料、建議保護政策，並協助更快地調查和修復資料安全性事件，最終讓資料安全性團隊能將更多時間和注意力放在策略性工作上。使用 AI 還能提升組織對於整體資料安全性策略的信心與滿意度，尤其是快速且準確回應事件的能力。

1

資料安全性景況仍然分崩離析，因此更需要具凝聚力的資料安全性策略，應對傳統與 AI 使用相關的新風險。

決策者對其資料安全性實務的信心與其資料的真正保護程度之間存在斷層

根據 2023 年的報告，絕大多數決策者對其資料安全性策略充滿信心，74% 的決策者表示在 2024 年對其目前的解決方案感到滿意。88% 的人認為他們知道大部分關鍵資訊的位置，85% 的人表示他們的資料已妥善分類和標示。大多數人也相信他們的防禦控制，79% 的人相信他們能夠防止資料外洩，76% 的人認為他們的方法是主動而非被動的。

然而，隨著事件嚴重性持續增加，他們的信心也受到考驗。**年度資料安全性事件的平均數從 2023 年的 166 件到 2024 年的 156 件，一直維持在高水平，而這些事件的嚴重性也從 20% 的嚴重事件增加到 2024 年的 27%。**

156

起資料安全性事件

27%

被視為嚴重事件的比例

(比 2023 年增加 20%)

63%

每天檢閱的警示數量

一家重型設備製造商的資訊治理資深經理表示:「軟體平台建立的地點、其資料儲存的地點，以及誰會存取這些資料，讓我們的 AI 工具和供應商的資料安全性和管理變得複雜。我們有超過 100 年的資料，必須依照我們營運所在的每個司法管轄區的法律要求加以保護和治理。」

資料安全性事件的嚴重性增加，也因此導致警示數量增加。**組織平均每天面對 66 個警示，比 2023 年的 52 個還要多。**這個數位因組織規模不同而有顯著差異，中型企業 (500-999 名員工) 和大型企業 (1,000-4,999 名員工) 平均每天會收到 56 個警示，特大型企業 (5,000 名以上員工) 則平均每天收到 80 個警示。

鑑於資料安全性警示的數量之多，大多數組織根本無法跟上也就不足為奇了。資料安全性團隊平均要檢閱 63% 的每日警示。這些警示中有 35% 是誤報。感知到的控制與實際作業之間的錯配，讓資料安全性團隊應接不暇 - 試著評估他們是否有正確的保護措施，或如何微調這些措施，同時又擔心潛在的嚴重事件可能會從縫隙中溜走。

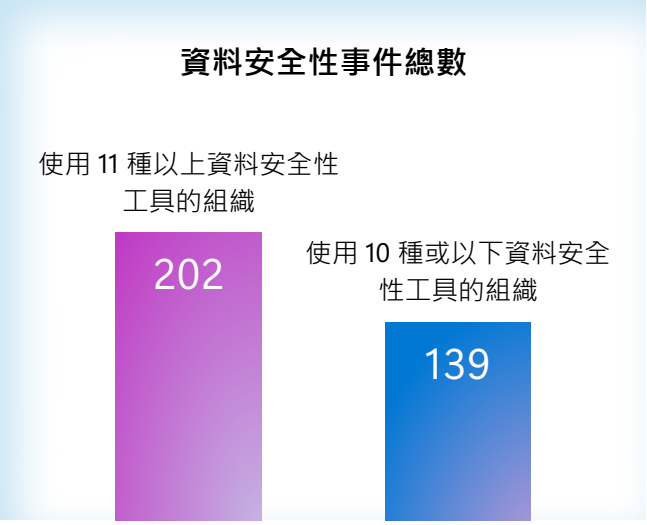
為了對抗與使用 AI 工具相關的傳統及新興資料風險，越來越需要更強大且具凝聚力的資料安全性策略

儘管可使用的工具越來越多，許多決策者仍然認為多不一定是好的。事實上，21% 的決策者認為他們最大的挑戰 / 風險是因為不同的工具所造成的缺乏整合且全面的可視性 (以及對風險的共同理解)。[1]

大多數決策者 (82%) 都同意，一個全面、完全整合的平台比管理多個獨立的工具更有優勢。**平均來說，他們要兼顧 12 種不同的資料安全性解決方案，這樣的複雜性使他們更家脆弱不堪。**這對於最大的組織來說尤其如此：中型企業平均使用 9 種工具，大型企業使用 11 種，而超大型企業則使用 14 種。

資料顯示，所使用的資料安全性工具數量與資料安全性事件發生頻率之間存在強烈的相關性。中型和大型企業平均每年報告 89 起事件，而特大型企業每年則面臨驚人的 248 起事件。這個明顯的差異突顯出大型企業所面臨的高風險，即使他們對自己的資料安全性措施表示相當有信心。

在 2024 年，使用較多資料安全性工具 (11 種或以上) 的組織平均會發生 202 起資料安全性事件，而使用 10 種或以下工具的組織則會發生 139 起事件。



分散的解決方案難以瞭解資料安全性勢態，因為資料是孤立的，而且不同的工作流程可能會限制潛在風險的全面可視性。當工具無法整合時，資料安全性團隊必須建立流程來關聯資料，並建立一致的風險觀點，這可能會導致盲點，使有效偵測和降低風險的工作變得困難。

一個日益令人關注的領域是，因使用 AI 應用程式而導致的資料安全性事件增加，從 2023 年的 27% 增加近一倍至 2024 年的 40%。這樣惡意軟體和勒索軟體攻擊的激增助長了事件的增加，從 2023 年的 50% 上升至 59%。來自使用 AI 應用程式的攻擊不僅會暴露敏感資料，也會危及 AI 系統本身的功能，讓原本就支離破碎的資料安全性情勢更加複雜。簡而言之，越來越迫切需要更強大和更有凝聚力的資料安全性策略，應對與使用 AI 工具相關的傳統和新興風險。

1. 2024 年 9 月對資料安全性、治理、合規性和隱私決策者進行的調查、治理、合規性和隱私權決策者進行的調查由 Microsoft 委託機構 MDC Research 進行研究

前進的道路

資料安全性事件嚴重性的增加，為 AI 提供了協助的機會。走在最前沿的組織正在實作 AI 驅動的資料安全性，協助進行事件優先次序排序、自動化資料分類以及找出微調現行保護政策的方法。AI 可以自動綜合事件警示的潛在嚴重性，為資料安全性團隊提供可快速回應的行動洞察力，減少花在誤判上的時間。這可簡化工作流程，讓資料安全性團隊能專注於更具策略性的資料安全性改善與主動措施。

2

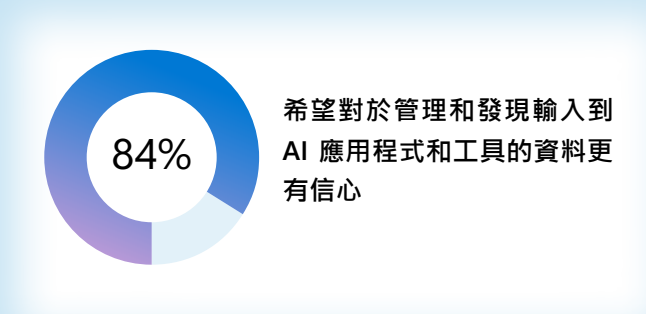
隨著終端使用者越來越多採用 AI 應用程式，組織最敏感資料的完整性面臨更大的風險，需要更多的可視性和新的保護控制措施

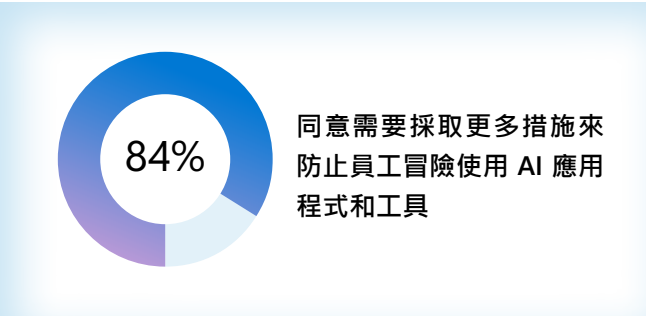
AI 正迅速成為日常工作的必要條件 - 而組織必須擁抱並積極適應此新現實

員工對 AI 工具的快速採用，促使組織對資料安全性的處理方式產生重大變化。雖然 AI 正在改變生產力和工作流程，但就像任何新興技術一樣，它也可能擴大現有風險或引進新的風險，因此需要不同的方法來保護敏感資訊。因此，企業仍在快速變化的環境中尋找立足點。一位運輸業的工程與分析總監表示：「在 AI 方面，我們對資料的監控更加謹慎。生產力與安全性、精確性與隱私權之間一直存在緊張關係」。

對於保障員工使用 AI 的信心仍是好壞參半。大多數人 (84%) 希望對管理和發現資料輸入更有信心。雖然有 22% 的組織對於保護資料安全性的能力極有信心，但大多數 (59%) 的信心僅限於「非常有信心」，顯示仍有改善的空間。大多數公司 (86%) 承認，他們希望更看好 AI 工具所產生的資料的管理與發掘。

隨著 AI 在日常生產力中變得越來越重要，AI 應用程式的使用也增加了對資料安全性事件的擔憂。**近三分之一 (31%) 的組織預計員工使用 AI 會導致資料安全性事件增加，84% 的組織承認需要採取更多措施來防範這些風險。**這種憂慮在最大的組織中尤其嚴重：26% 的中型企業預期與 AI 相關的資料安全性事件會增加，29% 的大型企業預測會增加，而 36% 的超大型企業預測會增加。





未經授權使用 AI 的情況非常普遍

40% 的人表示他們的 AI 應用程式已經在資料安全性事件中被攻破或洩露。同樣地，這個數位在大型企業中較高：中型企業報告的事件率為 36%，大型企業報告的事件率為 38%，而特大型企業的事件率最高，達到 44%。

員工使用個人憑證登入或使用個人裝置執行工作相關任務時，常會發生未經授權使用 AI 的情況。**平均而言，有 65% 的組織承認其員工正在使用未經授權的 AI 工具。**員工使用未經授權 AI 工具的方式包括：

- 53% 使用個人憑證登入工作用途
- 48% 的人在使用 AI 工作時使用個人裝置
- 47% 為了個人目的使用工作憑證使用 AI

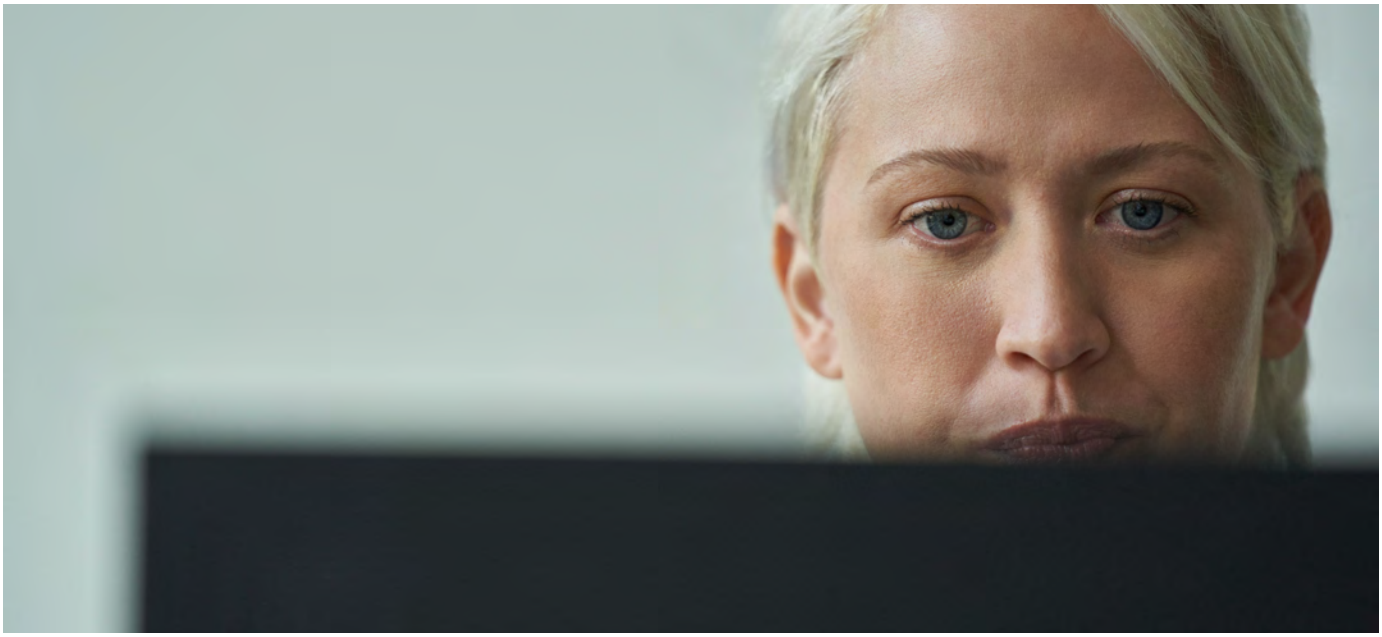
半數組織表示，他們擔心員工在以不安全性的方式使用 AI 應用程式時，缺乏偵測與降低風險的控制措施。這個數位因公司規模而異，43% 的中型企業、50% 的大型企業和 54% 的特大型企業對管理這些風險的能力表示憂心。

鑒於 AI 的使用越來越多，有必要採取更多資料安全性控管措施

隨著 AI 愈來愈深入日常運作，企業也意識到需要更強大的保護。**雖然 96% 的企業對員工使用這些工具有所顧慮，但幾乎同樣多的企業願意投資解決方案，克服他們的顧慮。**

「最大的焦點將是如何領先 AI ？安全性方面的重點在於減少資料的大小、更仔細地監控資料。在 AI 方面，為了讓您的模型更具代表性，找出偏差，您需要更多的資料。運輸業的工程、架構與分析總監表示：「那麼您要如何協調呢？絕大多數的決策者 (87%) 都準備好花時間與金錢，訓練員工使用 AI 工具的安全性實務。**這是因為 85% 的人表示，員工使用這些工具對保持競爭力至關重要。**

幾乎所有的組織 (93%) 都處於開發或實作 AI 使用控制的某個階段，但許多組織仍處於早期階段。只有 39% 的組織已針對 AI 全面實作資料安全性控管，24% 的組織已制定政策，但尚未付諸實行。一位服務業的資料安全性副總裁表示：「我們必須在 AI 的控制上作出調整，但同時也要接受 AI 的使用。它確實讓生活更美好，幫助我們提高效率。」



儘管企業正採取措施保護敏感資料，免在 AI 應用程式中被濫用，但顯然需要更全面的控制措施。目前，43% 的公司專注於防止敏感資料上傳至 AI 應用程式，另有 42% 的公司則記錄這些應用程式中的所有活動和內容，進行潛在調查或事件回應。同樣地，有 42% 的公司正阻止使用者存取未經授權的工具，另有相同比例的公司正投資於員工安全性使用 AI 的訓練。

員工未經授權使用 AI 的公司對特定類型的控制需求較高。**在未經授權使用 AI 的企業中，42% 需要控制措施，根據 AI 查詢識別有風險的使用者，而未經授權使用 AI 的企業則只有 30%。此外，在處理未經授權使用 AI 的組織中，有 40% 需要控制措施來管理資料的生命週期（例如保留與刪除協議），而沒有此問題的公司則只有 27%。**

需要的五大 AI 控制措施

防止敏感性資料上傳至 AI	43%
記錄 AI 工具中的所有活動和內容來進行潛在調查或事件回應	42%
阻止使用者存取未經授權的 AI 工具	42%
訓練員工安全性使用 AI 工具	42%
根據對 AI 的查詢識別有風險的使用者	41%

前進的道路

為了維持強大的資料安全性勢態，團隊需要一套完整的控制機制來發現、保護和管理他們在 AI 應用程式中的資料。以下是團隊可以使用的三個關鍵策略：

提高 AI 應用程式使用情況和流經應用程式的資料的可視性：利用可偵測和使用 AI 應用程式的資料安全性工具。這些工具可讓您深入瞭解正在使用的 AI 應用程式的全面清單以及其風險概況，包括支援的資料安全性控制和符合法規等詳細資訊。使用可為 AI 互動中的敏感資料提供一致分類的工具，並顯示資料如何流經 AI 應用程式的趨勢。

制定並執行政策：根據分析所得的洞察力建立政策。這些政策可包括核准 AI 應用程式的指引以及封鎖或限制員工使用未核准應用程式的程序。即使在核准的 AI 應用程式中，您也可以建立細部政策，允許非敏感性資料流通，同時限制使用敏感性和關鍵業務資料。這可包括封鎖某些動作，例如將敏感資料貼入瀏覽器型 AI 工具，確保資料安全性。

定期評估風險並完善政策：定期產生報告，顯示所使用的 AI 應用程式的風險等級、敏感資料流經這些應用程式的趨勢以及使用者圍繞這些應用程式的活動。這有助於評估整體風險狀況，並針對最相關的資料安全性政策做出明智的決策。

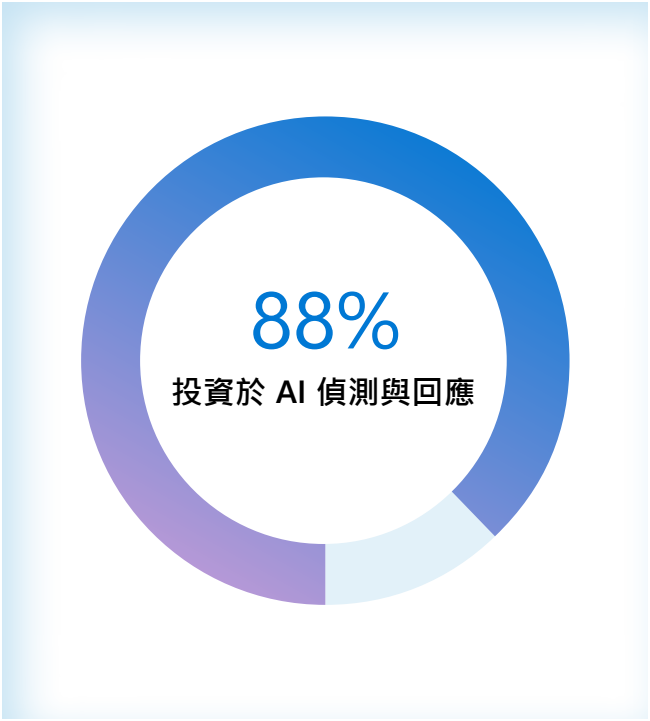
3

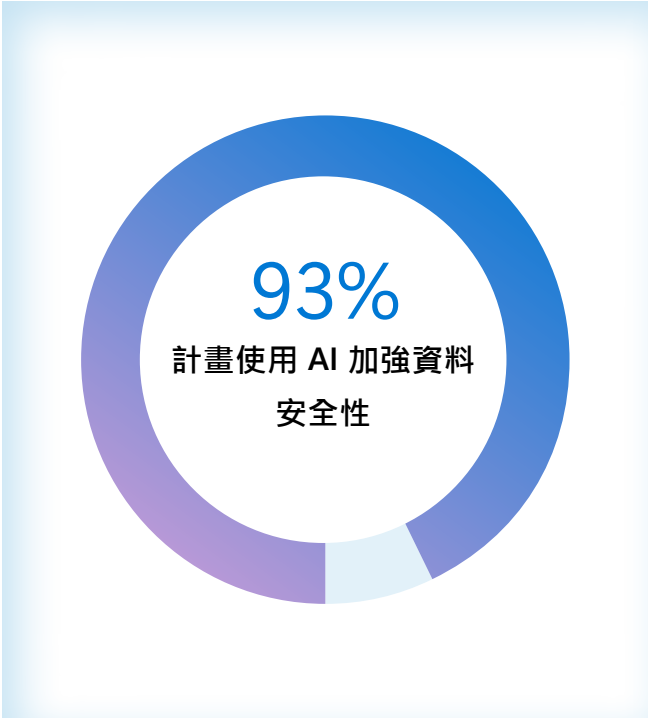
決策者對於 AI 提升資料安全性的潛力感到樂觀

資料安全性調查嚴重依賴 AI

絕大多數 (88%) 的組織已經在投資 AI，改善其偵測和回應工作 - 發現敏感資料、偵測異常活動以及自動保護有風險的資料。**77% 的組織認為 AI 將加速這些流程，76% 的組織認為 AI 將提高偵測與回應策略的準確度。**

雖然 73% 的決策者對於使用 AI 來強化資料安全性表示憂慮，但有 50% 的決策者表示這並未抑制他們使用 AI 來強化資料安全性，只有 23% 的決策者表示這已經讓他們卻步。總括而言，儘管存在疑慮，但絕大多數的 93% 至少仍計畫使用 AI 來強化資料安全性。



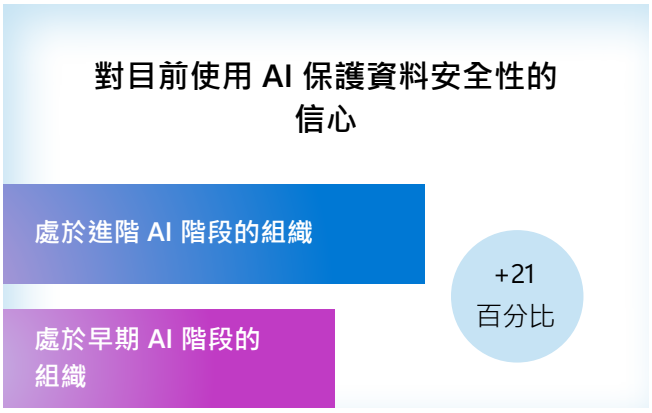


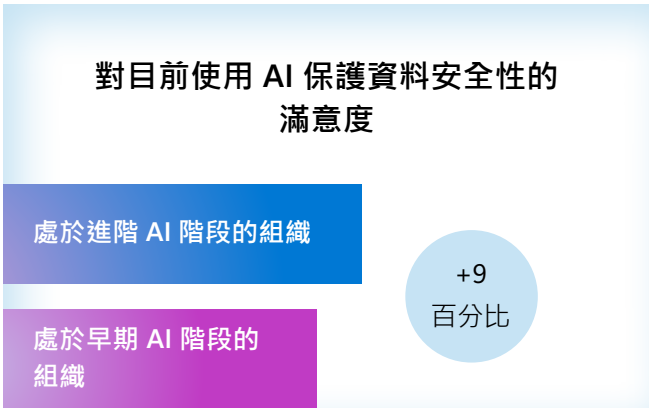
使用 AI 加強資料安全性可提高能見度、信心與滿意度

使用 AI 加強資料安全性的主要優點之一，就是能夠提高整個系統的可視性，減輕決策者對於資料儲存位置與分類方式的憂慮 (20%)。[1]88% 的資料安全性決策者認為，將 AI 整合到資料安全性解決方案中，將可讓團隊擁有更高的可視性，這將允許組織處理和分析遠比其他方式更多的資料。中型企業主要著重於降低短期風險，例如在資料安全性程序中盡量減少人為錯誤。事實上，有 43% 的中型企業將減少人為錯誤所造成的風險列為優先考量，相較之下，特大型企業僅有 37%。

相較之下，大型企業的方法較為先進，強調較長期的風險和適應性的需求。這種高度的複雜性讓資料安全性團隊能夠更好地適應不斷演變的風險 - 這是 49% 超大型企業的首要任務，而中型企業則只有 43%。

整體而言，在使用 AI 加強資料安全性方面進展較快的企業，對其資料安全性策略的信心與滿意度都較高。**在 AI 實作進階階段的企業中，有 90% 對於使用 AI 來強化資料安全性感到非常有信心或非常有信心，而在早期階段則只有 69%。同樣地，76% 已進階運用 AI 的組織對其資料安全性解決方案表示滿意，而早期階段的組織中只有 67% 表示滿意。**





1. Microsoft 委託 MDC Research 於 2024 年 9 月針對資料安全性、治理、合規性與隱私權決策者所進行的研究

組織利用 AI 減少資料安全性事件的發生，並改善警示管理

使用 AI 來強化資料安全性作業的組織所報告的警示顯著減少。**平均來說，已採用 AI 驅動資料安全性工具的組織每天會收到 47 個警示，而未採用 AI 驅動資料安全性工具的組織每天則會收到 79 個警示。此外，使用 AI 的組織能夠檢閱 66% 的每日警示，而未使用 AI 的組織只能檢閱 60%。**

此外，使用 AI 加強資料安全性的組織，也更有可能使用 AI 來降低風險 (56% 比 26%)。警示數量的減少以及利用 AI 緩解警示的能力提升，似乎對資料安全性事件的總數量產生了顯著的影響。與未使用 AI 來強化資料安全性的組織相比，已實作 AI 來強化資料安全性的組織，資料安全性事件減少了 65%。

預期 AI 對回應的影響最大

在偵測方面，33% 的決策者預期 AI 將有助於偵測異常活動，而 23% 則認為 AI 將協助調查潛在的資料安全性事件。另有 22% 的決策者認為 AI 有潛力提出建議，更好地保護資料環境。

然而，回應是決策者期望 AI 能產生最深遠影響的地方。34% 的人認為 AI 可以自動阻止敏感資料的不當分享，32% 的人表示 AI 可以保護有風險的資料。另有 26% 的人認為 AI 有助於降低資料安全性風險，並應用適當的控制措施，而相同比例的人則期望 AI 能自動標示有風險的使用者行為。

前進的道路

將 AI 整合到資料安全性解決方案中，可為團隊提供即時指引、總結功能和自然語言支援，突顯可能被忽略的區域。這也能加速調查，並加強資料安全性團隊的專業知識。以下是這些功能如何發揮影響力：

警示摘要：由於需要分析的來源數量眾多，且政策規則也各不相同，因此調查工作可能會相當艱鉅。透過在資料遺失防護 (DLP) 和內部風險管理 (IRM) 中嵌入 AI，團隊可以快速收到警示摘要，包括來源、政策規則和使用者風險洞察，瞭解哪些敏感資料遭到洩露以及相關的使用者風險。

前後關聯式溝通：組織必須遵守有關商業通訊的法規要求，這通常需要對違規行為進行廣泛的審查。AI 可協助資料安全性團隊依據法規和企業政策評估內容，突顯可能導致資料安全性事件的高風險通訊。

自然語言至關鍵字查詢：在調查過程中，搜尋可能是複雜且耗時的工作流程，通常需要使用關鍵字查詢語言。AI 可讓資料安全性團隊以自然語言輸入搜尋提示，簡化搜尋的開始，並進行更進階的調查。

最終的建議

1 採用整合式平台來對抗資料安全性事件

在日益演進的環境中，採用完全整合的資料安全性平台可提供更安全性、更精簡的策略，降低複雜性、增加能見度，同時改善防護。整合式方法可將資料安全性控制集中化，並提供統一的資料、使用者和活動可見性，協助組織改善資料安全性勢態管理，強化和簡化資料風險的偵測與防護。82% 的組織同意整合式平台更為優異，因此邁向整合不僅有益，更是必要之舉。

2 提高內部使用 AI 的能見度，以評估員工使用不影響生產力 AI 的必要控制措施

隨著 AI 在工作場所變得越來越普遍，它可能會放大現有的風險，並引入新的風險。組織承認他們需要採取更多措施來防止不安全性的 AI 使用。利用 AI 應用程式的內建控制與可視性，對於在不影響生產力的情況下維護資料安全性至關重要。訓練員工安全性使用 AI 可協助組織將風險行為降至最低，同時確保團隊能繼續從這些強大的工具中獲益。

3 在 AI 的協助下提升您的資料安全性策略

AI 可讓資料安全性團隊專注於更具策略性的計畫，而非回應持續不斷的威脅和大量警示。處於 AI 實作進階階段的公司，比起那些剛起步的公司，對於他們的資料安全性解決方案更有信心，也更為滿意。透過部署 AI 作為全面性資料安全性策略的一部分，組織可以提高其可視性，強化偵測和應對風險的能力，最終提升整體資料安全性勢態。

研究目標

研究目標包括：

1. 瞭解資料安全性狀況，包括優先次序和心態、挑戰以及資料安全性事件的因果關係。
2. 探索資料安全性的未來，包括哪些策略和創新以及組織打算如何投資未來。
3. 探索 AI 在提升資料安全性的作用以及 AI 在保護資料方面所扮演的角色。

方法

2024 年 8 月 5 日至 23 日，對 1,376 位資料安全性決策者進行了 20 分鐘的多國線上調查。

問題主要圍繞與 2023 年比較的資料安全性狀況和資料安全性事件。此外，今年的調查還包括圍繞保障員工使用 AI 以及使用 AI 加強資料安全性的問題。

受眾招募

為符合篩選標準，資料安全性決策者需為：

- CISO 及相鄰決策者 (C-2 及以上)，其權限包括資料安全性
- 任職於企業組織 (500 名以上員工；規模不一)
- 受規範與不受規範的產業 (無教育、政府或非營利組織)

在接受研究調查的 1,376 位資料安全性決策者中，依國家 / 地區劃分的完成人數：

- 美國：302
- 英國：305
- 印度：301
- 巴西：158
- 法國：156
- 澳洲：154

hypothesis Microsoft Security