Microsoft

hypothesis

資料安全性索引

鞏固資料安全的趨勢、見解和策略

前言

在資料激增的時代，組織的資料無異於其生命線，這已是日漸顯著的情況。組織建立和使用的大量資料為關鍵業務提供了動力，為策略和全球決策提供了資訊，並塑造了組織未來的可能性。資料不僅是種資源，更是現代企業的命脈。

然而，隨著對資料相依性的增加，嚴峻的現實是，數位黑暗面中的漏洞真實存在，並且正在迅速擴大。網路威脅、資料外洩和內部風險事件不再是罕見事件，它們無處不在且不斷升級，給依賴資料的企業帶來了風險。在我們最近調查的決策者中，有 89% 的人表示，他們認為資料安全性態勢對其整體成功至關重要。

在本白皮書中，我們將著手探討此根本要務：防護貴組織的資料。我和我的團隊很高興能與您分享我們的發現，並希望能就如何繼續共同推動資料安全性邁向卓越展開對話。我們的調查結果表明，資料安全性正處於關鍵時刻 - 雖然安全性決策者們都認為資料安全性對他們的資料安全至關重要，而且大多數人都表示他們對自己所做的工作充滿信心，但他們同時也遇到了大量的資料安全性事件和挑戰。而且，在我們採訪過的領導者中，有 80% 的人發現最佳的整合方法優於現成解決方案，但大多數公司仍在使用分散的多工具系統來保護資料，這往往會導致更多而不是更少的安全性事故。

請您閱讀和分享這份最新報告，並藉此與我們的團隊展開對話，瞭解如何更好地保護我們共同的未來。

Rudra Mitra
Microsoft 公司資料安全性與合規性部門副總裁

前言

防止資料外洩和其他安全性事件仍然是安全性和風險決策者持續關注的問題，也是任何網路安全性計畫的基石，因為一次外洩就可能造成重大的聲譽和經濟損失。企業的任務是保護各種敏感性資料，包括員工和客戶資訊、智慧財產權、財務預測和營運資料。

為了瞭解目前資料安全性做法和趨勢，並確定企業加強資料安全性的機會，Microsoft 委託獨立研究機構 Hypothesis Group 對 800 多名資料安全性專業人士進行了跨國調查。本報告介紹了研究的五大發現，包括資料安全性的趨勢、見解和策略。

重要發現

1

決策者認為他們受到了保護，但現實與認知並不相符。

雖然大多數決策者表示，他們對自己的資料安全性解決方案感到滿意並充滿信心，但他們仍然平均每年遭遇 59 起資料安全性事件，造成了高昂的損失。

2

擁有更多的工具並不代表資料安全性或效率的提高，情況恰巧相反。

有 80% 的決策者認為，全面整合的解決方案優於手動的業界最佳解決方案，但組織使用工具的方式仍然很分散，平均使用 10 種以上的資料安全性工具。但是，使用工具最多的組織也經歷了更多的資料安全性事件，這表明工具越多，安全性就越弱。

3

企業繼續受到外部和內部資料安全性事件的壓力困擾，尤其是業務資料。

有 50% 的受訪組織在過去一年中經歷過勒索軟體或惡意軟體攻擊，而許多決策者並不認為他們的企業已做好充分準備來預防和應對未來的勒索軟體或惡意軟體攻擊。從內部觀點來看，內神通外鬼是最令人擔憂的問題。此外，組織還高度關注其業務資料的脆弱性。這再次凸顯了全面應對風險的安全性平台的必要性。

重要發現

4

組織需要雲端和 AI 來推動數位轉型，但這也是最脆弱的資料位置。

雲端應用程式和 AI 技術已成為組織協作和提高生產力的關鍵，然而這種演變也帶來了更多動態和多方面的風險。隨著組織擁抱 AI，加強資料安全性以實現負責任的安全性使用變得至關重要。

5

自動化和 AI 是有望加強保護的絕佳途徑。

組織希望其團隊在偵測上花費更少的時間，在預防上花費更多的時間。自動化可以讓團隊將更多精力放在積極主動的措施上，而將 AI 用於資料安全性則可以協助組織更具策略性，更智慧地應對未來的威脅。

1

決策者認為他們受到了保護，但現實與認知並不相符。

決策者認為他們受到了保護，但現實與認知並不相符。

從表面上看，決策者對其資料安全性解決方案的信心和滿意度都很高，大多數組織都認為他們的資料安全性控制措施足以防止資料外洩，他們認為自己知道大部分資料存放在哪裡，並且能夠偵測到資料周圍的大部分風險。

與此同時，組織繼續經歷著大量的資料安全性事件 - 在過去 12 個月中平均發生了 59 起，其中五分之一被認為是「嚴重」事件。這些事件的影響範圍很廣，平均而言，組織估計最嚴重的資料安全性事件的總財務成本約為 24.4 萬美元，這代表每年的事件成本高達 1500 萬美元。除了這些成本外，十分之四的決策者還表示，資料安全性事件的恢復營運成本以及聲譽受損造成的業務損失也是他們高度關注的問題。

此外，有 92% 的決策者面臨挑戰，主要是在成本、整合和實作時間等方面，這阻礙了他們進一步投資資料安全性的能力，這表明需要更多預算友好型和勞動高效型解決方案。

對資料安全性準備程度的信心認知與組織所遭遇事件的實際情況不同。儘管對於企業來說，瞭解資料的位置和偵測風險非常重要，但這些措施單獨或分別採取，都不足以協助企業預防那些讓資料安全性和風險決策者徹夜難眠的事件。

正如金融服務業的資安長 (CISO) 所言：「我不能跟我的董事會說：『我確保了資料安全性，只是沒有做好防護』...我們最不希望看到的就是自家銀行的失敗消息出現在《華爾街日報》的頭版上。」

59

過去 12 個月資料安全性事件的平均數量

最高

1500 萬美金

嚴重安全性事件的年度成本

2

擁有更多的工具並不代表資料安全性或效率的提高，情況恰巧相反。

擁有更多的工具並不代表資料安全性或效率的提高，情況恰巧相反。

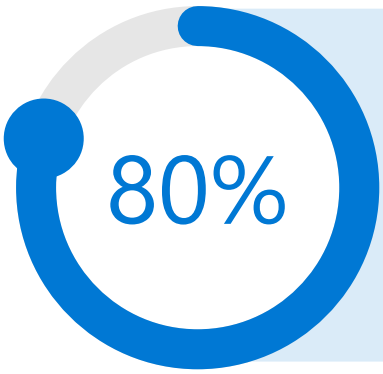
各組織逐漸意識到，由於資料安全性工具各自為政，多年來採用的現成解決方案方法在可見度和效率方面造成了落差。有 80% 的組織認為，使用整合解決方案的綜合資料安全性平台要優於使用多個必須手動整合和管理的業界最佳解決方案。

儘管絕大多數組織認為整合解決方案更優越，但資料安全性工具的使用卻非常分散。

因此，組織平均使用 10 種資料安全性工具來應對資料安全性風險，包括資料遺失防護、資訊保護、內部風險管理、安全性資訊與事件管理 (SIEM)、雲端存取安全性代理程式等。對於員工人數超過 5000 人的組織來說，工具的平均數量甚至更多。

擁有更多工具可能會產生虛假的安全感，因為與使用較少工具的組織相比，使用較多工具 (16 種以上) 的組織對其資料安全性狀況更有信心 (61% 對比 56%)。

然而，研究結果卻與這種安全性感相矛盾，因為使用 16 種或更多工具的組織在過去一年中也經歷了更多的資料安全性事件 - 平均 133 起，而使用較少工具的組織僅經歷了 48 起。



同意使用整合解決方案的綜合安全性平台優於使用必須手動整合和管理的多個同類最佳解決方案。

2.8 倍

去年發生的資料安全性事件更多

使用 16 種或更多工具的組織 (與使用較少工具的組織相比)

如果研究一下傾向於使用業界最佳解決方案或更多工具的觀點和做法，就會發現透過更多整合解決方案和更少工具來提高資料安全性的理由更加充分。

「如何從眾多系統中收集、彙總和使用資料？許多不同的資料點需要整合到生態系統中才能真正發揮作用。否則，您的資料安全性就真的跟瑞士乳酪一樣漏洞百出了。」

製造/生產部門
IT 副總裁

首先，多種不同的資料安全性工具會導致可見度方面的差距和更多的幽靈資料。事實上，關注幽靈資料者更偏好採用業界最佳解決方案。這很可能是因為採用業界最佳方法的組織需要付出更多努力，才能全面瞭解其資料安全態勢。

其次，管理孤立的解決方案會為資料安全性團隊帶來更多複雜性，因為每個不同的解決方案都需要專門的人員、安裝和維護端點代理程式，以及各種新流程。以警示審查和分級為例，這是需要人員和資源的任務之一。警報數量的增加代表資料安全性團隊在管理孤立的解決方案時需要付出額外的心力。使用較多工具的組織平均每天會收到 96 個資料安全性警示，而使用較少工具的團隊每天只收到 44 個，還不到一半。此外，他們無法與工具較少的團隊一樣審查那麼多的警示數 (61% 對比 68%)。與使用較少工具的組織相比，使用較多工具的組織往往更被動。

最後，更多的工具還表明，組織必須花費大量精力來整合見解和補救計畫，而且資訊可能會在轉譯過程中遺失。在提及資料安全性的最大挑戰時，實作或維護資料安全性解決方案的成本以及整合資料安全性解決方案的挑戰被列為前兩項。

這代表流程更長、更慢，在使用 16 種或更多工具的組織中，有 37% 的組織表示需要一個月或更長時間才能完成資料安全性調查，而在使用較少工具的組織中，此比例僅為 21%。

製造和生產部門的基礎結構與營運總監說道：「我們現正緩步進行中。我們擁有的每個系統都有自己的入口網站、工具與處理方式。每個人在自己專精的領域採用自己的方式。然後，他們再聚在一起，決定到底發生了什麼，我們再從那裡開始處理。因此，目前還需要人工作業。」

最終，由於選擇繼續使用多種解決方案，組織忽視了自己對整合解決方案優越性的理解，走向了相反的方向 - 耗費了時間和金錢。

使用較少 (<16 個) 和較多 (16 個以上) 資料安全性工具的結果	工具數量低	工具數量高
過去 12 個月**資料安全性事件**的平均數量	**48**	**133**
嚴重資料安全性事件的比例	**19%**	**26%**
我們目前的資料安全性策略多採用**被動式反應**	**31%**	**40%**
面臨**整合**解決方案的挑戰	**24%**	**39%**
資料安全性團隊將大部分時間用於**應對**	**19%**	**26%**
我們對自己的資料安全性態勢**有信心**	**56%**	**61%**
平均每天**收到**的警示數量	**44**	**96**
我們每天可**審查**的警示比例	**68%**	**61%**
完成資料安全性調查需要一個月或更長時間	**21%**	**37%**

3

企業繼續受到外部和內部資料安全性事件的壓力困擾，尤其是業務資料。

組織繼續受到外部和內部資料安全性事件的壓力困擾，尤其是業務資料。

由於與資料相關的因素 (包括與資料互動的人員、與資料相關的活動以及用於處理資料的裝置和應用程式) 在不斷變化，資料安全性事件和資料外洩隨時隨地都可能發生。而且，這些威脅既來自外部攻擊者，也來自可信賴的人員，包括員工、承包商和合作夥伴。無論是惡意還是無意，所有參與者都可能造成資料安全性事件，這代表需要在多個領域持續提供防護。

有位金融服務業的 IT 副總裁說道：「您要防護的東西總是不斷變化。這是會不斷移動的目標。它總是在發展、變化並且具有彈性。您要防護的東西以及其生存環境只會變得越來越多。」

雖然資料安全性事件可能來自不同來源，但惡意軟體或勒索軟體事件 (惡意軟體滲入系統，為攻擊者提供未經授權的系統或網路存取權) 的外部威脅最常見，有 50% 的受訪組織在過去一年中至少經歷過一次。

此外，這些攻擊也是組織感到最脆弱的地方，有 41% 的組織表示，他們認為自己在未來一年內應對惡意軟體或勒索軟體攻擊的準備最不充分。在那些傾向於採用業界最佳方法的組織中，這種脆弱感更加強烈 - 有 44% 的組織認為自己對此類攻擊毫無準備，相較於偏好採用整合解決方案的組織中，這種比例僅為 36%。

防範內部風險也是決策者最關心的問題。有 35% 表示，他們需要加強對惡意內部人員和外洩帳戶的防禦，三分之一的人對無意中發生的內部人員事件表示擔憂。雖然惡意內部人員事件可能不是資料安全性漏洞的主要原因，但卻是決策者認為最不容易防範的第二類事件。

「我每個月至少會接到一次主管驚慌失措打來的電話...『我們有個事件，我發現了有事件，或者威脅團隊發現有事件。』其中有些是無意的，有些是員工不知道或不瞭解他們的權限允許什麼行為。」

美國政府資安長

內部人員是受信任的個別人士，他們通常獲權存取公司資源、資料或系統權限，或擁有這些資源、資料或系統的知識，而這些資源、資料或系統一般不對公眾開放。因此，與內部人員相關的資料安全性風險通常更加難以捉摸和偵測。如 Microsoft 資安長 Bret Arsenault 所言：「歸根究底，入侵是有意還是無意並不重要。內部人員風險計畫應該成為每家公司安全性策略的一部分。」

資料安全性事件總結

資料安全性事件的原因	過去 12 個月中最常見的事件	未來 12 個月最未妥善防範的事件
惡意軟體或勒索軟體	50%	41%
遭入侵的帳戶	38%	35%
拒絕服務 (DoS) 的攻擊	35%	33%
失職的內部人員	32%	29%
意外犯錯的內部人員	31%	32%
惡意犯錯內部人員	31%	35%
實體財產	29%	29%

組織選擇的資料安全性解決方案還必須適用於各種敏感性資料，包括高價值業務資料、營運資料和個人資料。在過去 12 個月發生的資料安全性事件中，74% 的組織的業務資料被暴露，65% 的組織的營運資料被外洩，58% 的組織的個人資料易受攻擊。在各類資料中，智慧財產權、IT 和網路設計以及 PII 被外洩或暴露的情況最為常見。

展望未來，有 77% 的組織認為智慧財產權和原始程式碼等業務資料最容易受到攻擊。這主要是因為業務資料在建立競爭優勢和創收方面發揮至關重要的作用。然而，對這些資料進行識別和分類可能具有挑戰性，因為傳統的模式識別、規則運算式或函數匹配技術可能無法有效識別缺乏特定字串格式或關鍵字的內容。因此，組織需要更先進的技術來幫助發現和保護這些易受攻擊的敏感性資料。

未來 12 個月面臨最大風險的資料類型

77% 商務資料		64% 營運資料		63% 個人資料	
智慧財產權	30%	IT 和網路設計	29%	個人身分識別資訊 (PII)	31%
原始程式碼	28%	財務報表	18%	人力資源資訊 (薪資單、簡歷等)	21%
商務方案	27%	銷售和收入報告	15%	支付卡產業 (PCI) 資料	18%
商業機密	24%	採購和發票	12%	受保護的健康資訊 (PHI)	18%
併購檔案	20%	法務文件/協議	12%	認證	17%
施工規範	18%	製造程序/批次檔案	11%		

4

組織需要雲端和 AI 來推動數位轉型，但這也是最脆弱的資料位置。

組織需要雲端和 AI 來推動數位轉型，但這也是最脆弱的資料位置。

透過雲端應用程式和平台進行協作，再加上新的 AI 技術，可大幅提高員工的工作效率，實現彈性的工作安排，因此雲端應用程式和 AI 技術對組織來說至關重要。組織目前平均使用 147 種公共雲服務，涵蓋 SaaS、PaaS 和 IaaS。[1]而且，有 66% 的組織已制定 AI 策略，其中 36% 已經開始實施。[2]

現在，為這些高生產力資料位置提供正確的資料安全性解決方案變得更加重要。在過去的 12 個月中，有 42% 的組織報告了雲端儲存方面的安全性事件，有 31% 的組織報告了電子郵件、即時訊息或線上會議工具方面的安全性事件。在生產力和協作最高的地方似乎最容易發生安全性事件。

管理這些類型的事件需要資源，有 79% 的組織表示其資料安全性團隊需要更多人員來有效管理關鍵資料安全性責任。然而，在聲稱需要更多人員的組織中，大多數 (57%) 更偏好採用業界最佳的方法。這種偏好表明，使用更多解決方案的組織可能更難以在眾多使用者活動中識別真正的風險。

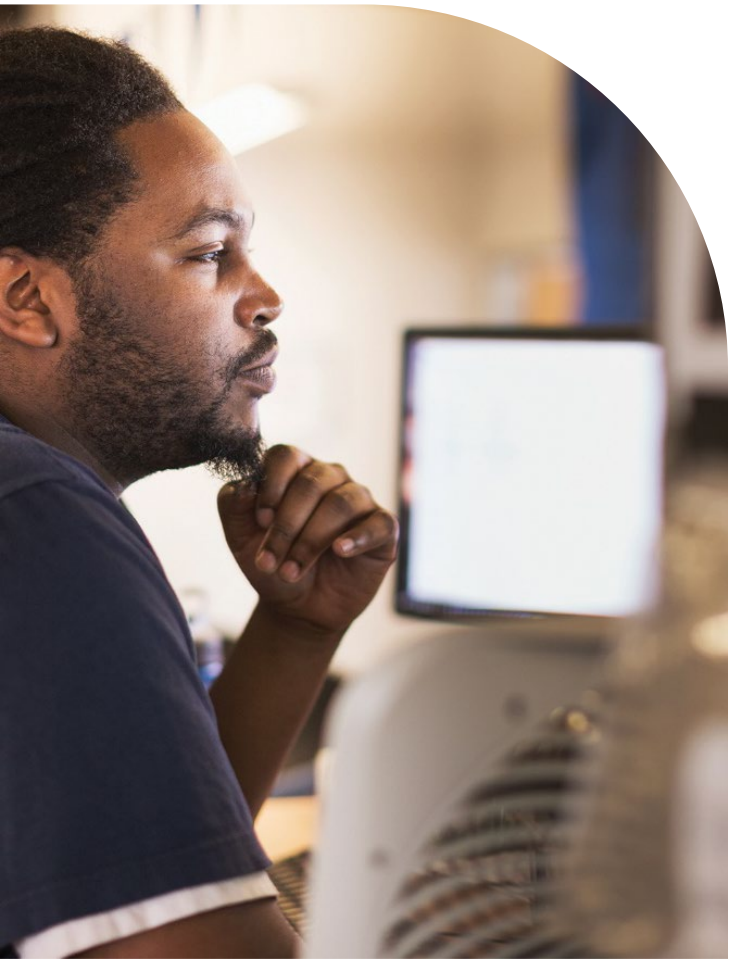
1.《衡量風險和風險治理》(Measuring Risk and Risk Governance)，雲端安全性聯盟 (Cloud Security Alliance, CSA)，2022 年。

2. Microsoft 資料安全性 AI 研究，Hypothesis，2023 年 3 月

資料位置總結

資料位置	在過去 12 個月中遭到入侵	風險最大
雲端儲存 (例如 Box、OneDrive、Google Drive)	42%	54%
電子郵件/即時訊息/線上會議工具	31%	39%
平台即服務 (PaaS)	29%	34%
基礎結構即服務 (IaaS)	28%	36%
AI (例如 ChatGPT、Bard 等技術)	27%	38%
基於 SaaS 的資料庫/資料湖	27%	41%
端點/裝置	25%	36%
內部部署存放庫/檔案共用/資料庫	24%	28%
幽靈資料	21%	23%
業務範圍應用程式	17%	25%
開發人員工具	16%	23%

超過三分之一的組織正在實作 AI 策略，而且還有更多的組織正在實作此策略，AI 正在以前所未有的速度獲得採用，速度遠超越過去採用雲端和電子郵件的速度。隨著組織開始採用 AI，加強資料安全性以實現負責任的使用和預防風險變得至關重要。與其他位置相比，AI 被認為是資料安全性事件的高危地點，有 27% 的組織經歷過 AI 資料安全性漏洞。組織對 AI 使用風險的擔憂主要集中在對與 AI 共用的資料缺乏控制、缺乏偵測和降低 AI 使用風險的控制措施、 AI 生成模型的訓練方式缺乏透明度，以及透過 AI 外洩機密資訊等方面。



「AI 有利於提高生產力和效率，但也存在潛在的安全性和資料風險。」有間組織的安全性決策者表示，

雖然存在對 AI 的擔憂，但決策者也看到了 AI 的潛力，尤其是市場上的供應商正在開發創新產品，透過負責任地使用 AI 來幫助組織增強能力。然而，為了進一步利用 AI ，組織報告說，他們需要的最主要控制措施是偵測 AI 中的惡意或風險內容，在資料上傳到 AI 之前對其進行加密、遮罩或匿名處理，以及識別 AI 生成的敏感性資料。

AI 所需的 5 大資料安全性控制措施

1. **偵測** AI 中**的惡意或風險性內容**
2. **在資料上傳到 AI 之前對其進行加密、遮罩或匿名**處理
3. **識別** AI 生成的敏感性資料
4. **防止敏感性資料上傳**至 AI
5. **偵測** AI 中**的模型順序資料操作**

5

自動化和 AI 是有望加強保護的絕佳途徑。

自動化和 AI 是有望加強保護的絕佳途徑。

在沒有組織優先順序或預算限制的理想情況下，半數組織希望在資料安全性管理方面更加積極主動，在發現敏感性資料及其相關風險和預防資料安全性事件等方面花費更多時間。但目前，有一半以上的組織將最多的時間花在了事件偵測、回應和調查等被動措施上。而對資料安全性事件的偵測和回應是時間密集型的 - 大多數組織需要大約一個月的時間來解決資料安全性事件，有些組織甚至需要長達六個月的時間來解決。

採取更加積極主動的策略的好處顯而易見，因為在接受調查的組織中，更加積極主動的組織遇到的資料安全性事件的成本更低，更有可能在不到一個月的時間內對這些事件進行調查，並且更有可能認為他們的防禦控制措施足以防止資料外洩。

雖然組織意識到積極主動的資料安全性措施有助於降低資料安全性風險，但在實作這些措施方面卻沒有取得進展。例如，希望透過分配更多時間進行預防來提高主動性的組織更傾向於選擇業界最佳的解決方案，而在將偵測訊號和回應控制結合在一起時，這些解決方案實際上要求在處理被動措施方面付出更大的努力。

組織對比結果：更積極主動與更消極被動

	更積極主動	更消極被動
過去 12 個月資料安全性事件的平均成本影響	**20.7 萬**	**3.3 萬**
平均在一個月內完成資料安全性調查	**80%**	**68%**
我們的防禦控制足以防止資料外洩	**77%**	**68%**

由於資源和人員有限，各項活動之間的精力分配可能並不理想，因此組織正在尋求技術來幫助他們留出更多時間開展積極主動的活動。自動化是組織騰出時間更積極主動地保護資料安全性的方法。有 74% 的受訪組織傾向於採用半自動或全自動的風險緩解措施，與人工審查相比，這可以讓安全性團隊提前將潛在資料安全性事件的影響降至最低。此外，組織還認識到許多其他任務也可以從自動化中受益，例如建立資料安全性報告、事件管理工作流程自動化以及事件回應和調查。安全性團隊希望自動化的首要任務大多是反應性措施。透過自動化這些任務，組織可以減輕資料安全性團隊的負擔，使他們能夠採取更加積極主動的態度。

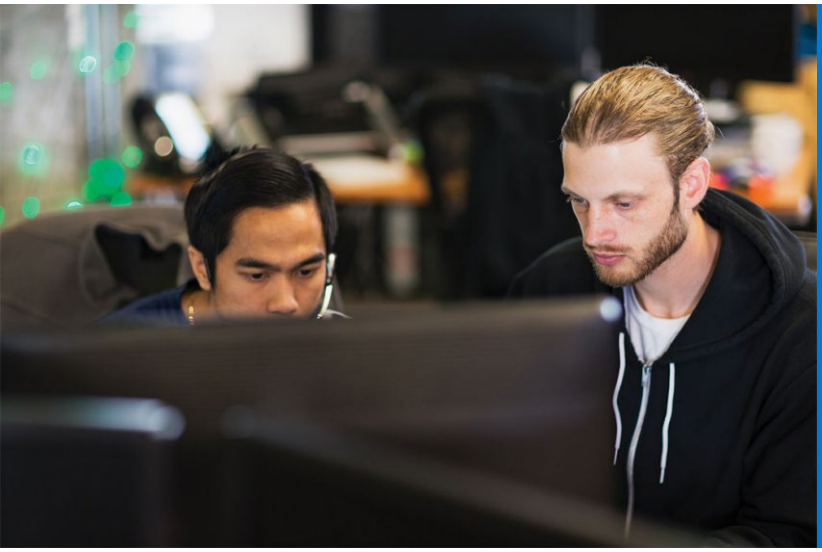
資料安全性團隊希望自動化/減輕負擔的 5 大領域

消極被動

1. 為事件管理和回應建立自動化工作流程
2. 建立資料安全性報告

消極被動

3. 應對和控制資料安全性事件
4. 在調查期間將事件轉給正確的團隊 (例如 SOC、法律、人力資源)
5. 調查資料安全性事件



「有太多的風險資料需要人工評估。AI 可以協助我們加快團隊的回應速度，並在資源不足的情況下保護資料。」

英國安全性決策者

將 AI 用於資料安全性還能協助組織更具策略性，更智慧地應對未來的威脅。該技術可加快對偵測到的事件的回應速度，為資料安全性專業人員贏得進一步調查的時間。與自動化類似，組織也列舉了許多 AI 可以幫助提供更強安全性情境，**節省團隊的時間**。AI 的主要應用情境包括自動阻止不適當的資料共用、偵測關鍵資料安全性風險/異常資料活動以及調查潛在的資料安全性事件。

透過利用 AI 和自動識別的優勢，並採用整合度更高的解決方案，組織可以採取更加積極主動的資料安全性策略，並為更安全性的未來做好準備。

AI 的主要應用情境

自動封鎖不適當的資料共用

偵測關鍵資料安全性風險/異常資料活動

更好地保護資料環境安全性的建議

調查潛在的資料安全性事件

完善資料安全性政策

最終的建議

- 採用整合平台加強資料安全性態勢
- 採用深度防禦方法，防範由外而內和由內而外的資料安全性事件
- 利用 AI 和自動化升級資料安全性策略

採用整合平台加強資料安全性態勢

根據這項研究的結果，更少的解決方案可以帶來更多的安全性。這似乎有悖常理，但組織必須消除因眾多孤立的解決方案而產生的虛假信任感。供應商整合提供了策略方法，不僅能降低成本，還能增強安全性。

資料安全性決策者可以透過授權其團隊將更多時間用於研究和規劃新的安全性控制以及最佳化安全性政策等策略性工作來啟動此轉變，84% 的決策者都認為他們希望這樣做。此程序包括替換傳統的孤立解決方案，這些解決方案通常被認為是「業界最佳」，但卻無法與其他工具有效整合。

決策者可以與其團隊密切合作，制定資料安全性計畫目標和關鍵績效指標 (KPI) 。然後，他們可以透過定義解決方案需求和確定不可協商的功能來取得進展。這種方法使他們能夠找到能夠提供符合其總體目標的工具的供應商。最重要的是，這種方法促進了前瞻性思維，幫助團隊避免過度固守現有做法或孤立的使用案例，使他們能夠實作必要的變革，採用更加整合的方法。

整合式資料安全性平台應使安全性團隊能夠無縫完成所有這些關鍵任務：

1. 發現並保護數位環境中的敏感性資料。
2. 偵測與這些資料相關的關鍵風險。
3. 防止未經授權使用敏感性資料，同時不影響合法業務活動。

透過實作綜合資料安全性策略，組織可以實現更高層級的保護，同時簡化其安全性基礎結構。

採用深度防禦方法，防範由外而內和由內而外的資料安全性事件

資料安全性事件通常由外部攻擊者、惡意內部人員或疏忽大意的內部人員造成。組織必須採取措施保護資料安全性，既要防止來自外部威脅的未經授權的存取，又要降低內部人員竊取或意外暴露資料的風險。

為了應對這些挑戰，組織可以採用深度防禦的方法來保護資料安全性。此策略類似於博物館對無價藝術品的保護：配備威脅情報的尖端安全性攝影機監控訪客、票務系統管理身分和進出博物館的權限，圍繞藝術品的嚴格安全性措施與保護您寶貴資料的資料安全性控制措施類似。這些措施可以阻止潛在事件的發生，無論是來自外部的壞人還是組織環境中的個人。

要應對不斷變化的資料安全性風險，需要整個組織齊心協力實作這種深度防禦策略。資料安全性團隊與安全性營運中心 (SOC) 等其他部門的合作可以最佳化資料安全性投資。值得注意的是，有 66% 的組織認為自己積極主動，與之相比，有 54% 的組織認為自己並非如此。

與安全性團隊之間的團隊合作一樣，資料安全性解決方案也應與其他系統無縫整合，例如擴展偵測和回應 (XDR) 或身分和存取管理 (IAM) 解決方案，有效防止來自外部和內部的資料安全性事件。透過這些整合，組織能夠對安全性事件進行全面調查和回應，徹底瞭解受影響的資料、行為者和活動，並透過多種緩解控制措施做出回應。因此，這使他們能夠做出明智、準確和及時的反應，充分減少潛在安全性事件的影響。

利用 AI 和自動化升級資料安全性策略

自動化和 AI 可以協助組織在資料安全性方面更加積極主動。以下是一些建議，供您的組織踏上自動化和 AI 之旅：

- 發現敏感性資料：利用 AI 協助識別敏感性資料並套用保護策略，包括加密和權限管理。這對於透過傳統模式識別技術難以偵測的業務資料尤為重要。組織可以利用機器學習或 AI 驅動的分類器等分類技術，這些技術以其智慧性和根據資料關聯內容或業務類別快速定位敏感內容的能力而著稱。此外，組織還可以採用精確的資料匹配技術來發現營運性或個人資料。

  此外，隨著產業法規 (例如 GDPR、HIPAA 或 PCI DSS) 的發展和資料環境的不斷變化，擁有可自訂且容易適應的高級分類技術以識別新類別的敏感性資料至關重要。保護敏感性資料：

- 偵測關鍵資料安全性風險：利用 AI 的力量，準確定位與敏感性資料相關的關鍵風險，並策略性地分配資源，應對潛在的高風險事件。AI 技術可以生成高可信度警示，讓安全性團隊節省寶貴的時間，否則這些時間可能會花在篩選大量誤報警示上。此外，AI 還能幫助組織識別難以捉摸的風險，尤其是當惡意行為者試圖逃避偵測時。當務之急是利用機器速度來超越這些威脅行為者。

- 動態預防資料安全性事件：利用 AI 和自動化，根據評估的風險自動定制預防和緩解控制措施，實現更具適應性和前瞻性的資料安全性策略。當 AI 驅動的解決方案偵測和評估風險時，自動預防控制可以迅速參與保護資料，緩解控制精確應用到高風險領域。例如，當高風險使用者偵測到資料外流意圖的早期跡象時，組織就可以套用更嚴格的資料遺失防護 (DLP) 策略，積極防範潛在的資料安全性事件。

希望本報告中的見解和建議有助於您增強資料安全性態勢，使貴組織能夠抵禦不斷變化的風險。

若要瞭解有關 Microsoft 資料安全性的更多資訊，請造訪 https://aka.ms/DataSecurityNews

詳細的研究目標、方法和受眾招募

研究目標包括：

1. 瞭解資料安全性狀況，包括優先事項、心態和挑戰
2. 繪製資料安全性事件的因果關係圖，確定資料安全性團隊可採取的行動，增強資料安全性態勢
3. 探索資料安全性的未來，包括圍繞將 AI 用於資料安全性的新興策略和創新

調查方法：

2023 年 7 月 28 日至 8 月 9 日，對 822 位資料安全性決策者進行了 15 分鐘的跨國線上調查。

問題主要圍繞資料安全性情勢、資料安全性團隊如何分配資源、資料安全性事件以及對資料安全性人工智慧 (AI) 的心態和使用。

為滿足篩選標準，資料安全性決策者必須是：

CISO 及鄰近決策者 (C-2 及以上)，擁有資料安全性 Purview

就職於企業組織 (500 名以上員工；規模不一)

受監管和非受監管產業的混合 (不包括教育、政府或非營利性產業)

在接受調查的 822 位資料安全性決策者中，依國家/地區分列的完成情況如下：

美國	329
英國	322
澳大利亞	171