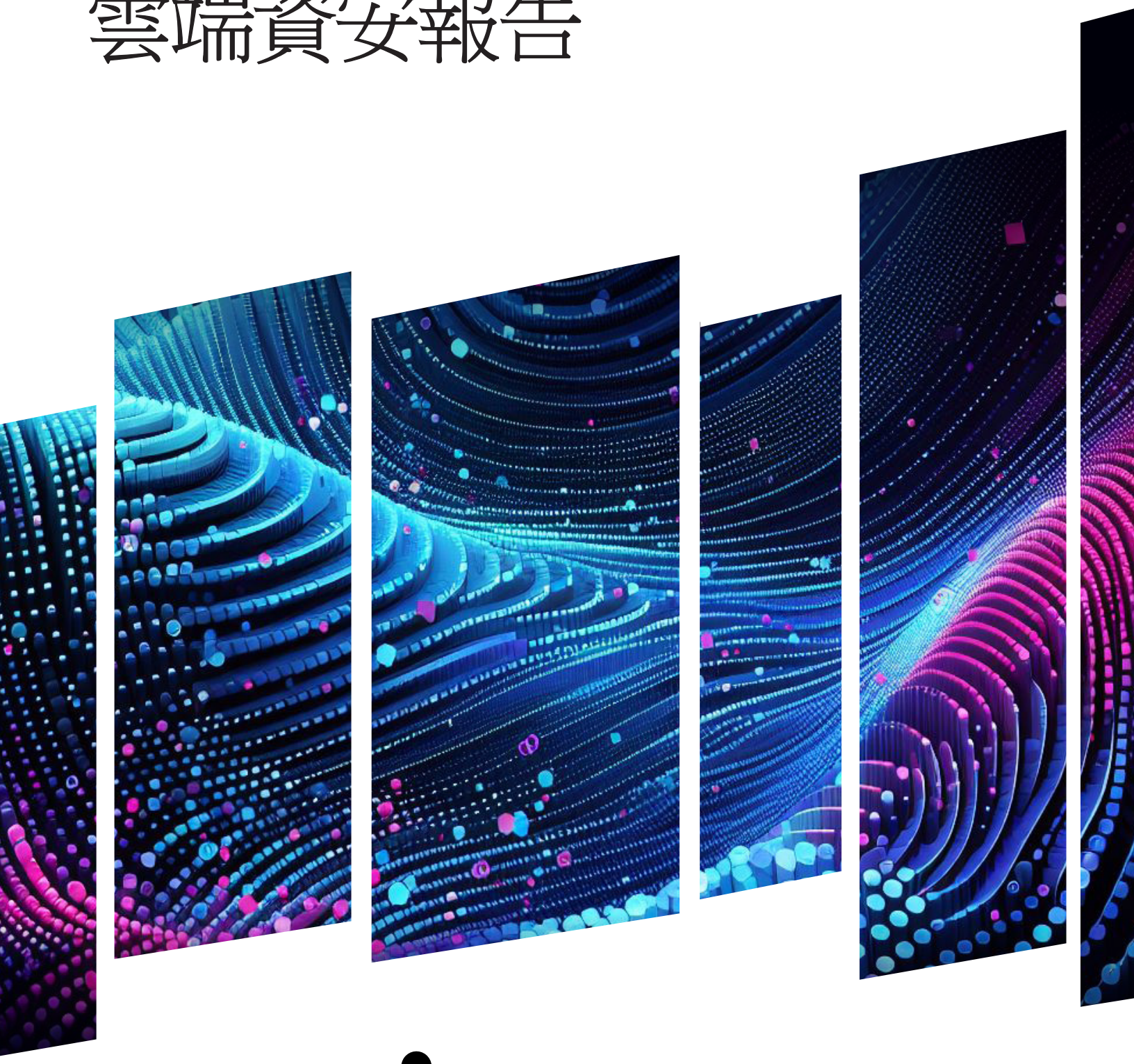
Cybersecurity
INSIDERS

2024 年
雲端資安報告



CHECK POINT™

簡介

隨著企業越來越依賴雲端技術，雲端平台的安全性已升級為重大問題，凸顯了其潛力和易受影響性。傳統資安措施往往不足以應對雲端環境所面臨威脅的動態和複雜性質，因此資安策略必須從被動應對轉向預防。

這份《2024 年雲端資安報告》揭示了雲端資安的迫切問題和不斷變化的首要事項。透過收集 800 多位雲端和網路安全專業人士的見解，本調查探索了雲端資安的現狀、現有安全措施的有效性，以及進階安全解決方案的採用情況，為此關鍵領域的挑戰和進展提供了全面看法。

主要調查結果包括：

- **安全事件不斷升級：**雲端資安事件正令人震驚地增加，去年有 61% 的組織報告發生過入侵，較前一年的 24% 顯著增加。此趨勢凸顯出雲端環境中不斷升級的風險格局。
- **入侵類型不斷變化：**資料安全外洩已成為最常見的雲端資安事件，有 21% 的組織報告遇到此問題。這種轉變凸顯出威脅性質的不斷演變以及保護敏感資料的迫切需求。
- **應對零時差威脅：**應對零時差威脅仍然是首要問題，91% 的受訪者擔心其系統是否有能力應對此類未知風險。此調查強調需要針對這些複雜攻擊建立預測性和即時防禦機制。
- **安全重點轉移：**儘管事件數量增加，但僅 21% 的組織優先考慮旨在阻止攻擊發生的預防措施。這顯示目前的雲端資安策略存在顯著的預防缺口。
- **CNAPP 採用加速：**雲端原生應用保護平台 (CNAPP) 的採用正在增加，25% 的組織已實施 CNAPP 解決方案。此趨勢反映了向整合預防、偵測和回應能力之全面安全措施的策略轉變。

我們衷心感謝 Check Point Software Technologies Ltd. 對本次調查的寶貴貢獻。他們的專業知識和支援有助於闡明現代雲端資安的複雜性和必要性。

我們希望本次調查所得出的見解，能成為致力於增強雲端環境安全性之組織的重要資源。

謹此致謝，

Holger Schulze

Cybersecurity Insiders 創辦人

Cybersecurity INSIDERS

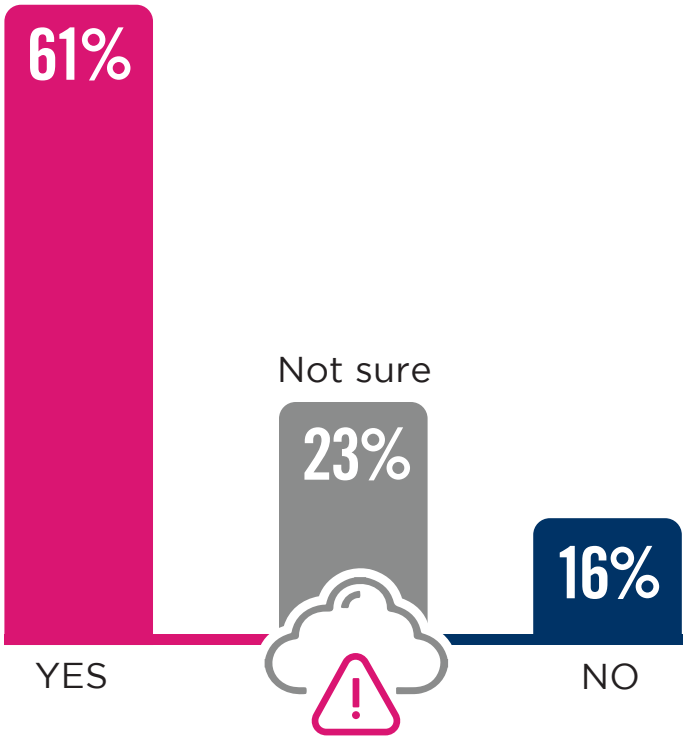
雲端資安事件不斷增加

了解雲端資安事件的頻率和性質對於掌握雲端環境中持續存在的脆弱性非常重要。

令人震驚的是，**61%** 的組織報告在過去 12 個月內經歷過雲端資安事件，較前一年的 24% 顯著增加。這種急劇上升凸顯出與雲端環境相關的風險，並強調迫切需要增強安全架構，優先考慮全面的可見性和主動威脅管理。

此外，**23%** 的受訪者不確定或無法透露有關這些事件的細節，這點顯示雲端資安令人擔憂地缺乏可視性和控制，這可能會加劇未被發現之入侵行為的風險。

Has your organization experienced any security incidents related to public cloud usage in the last 12 months?



重要見解：

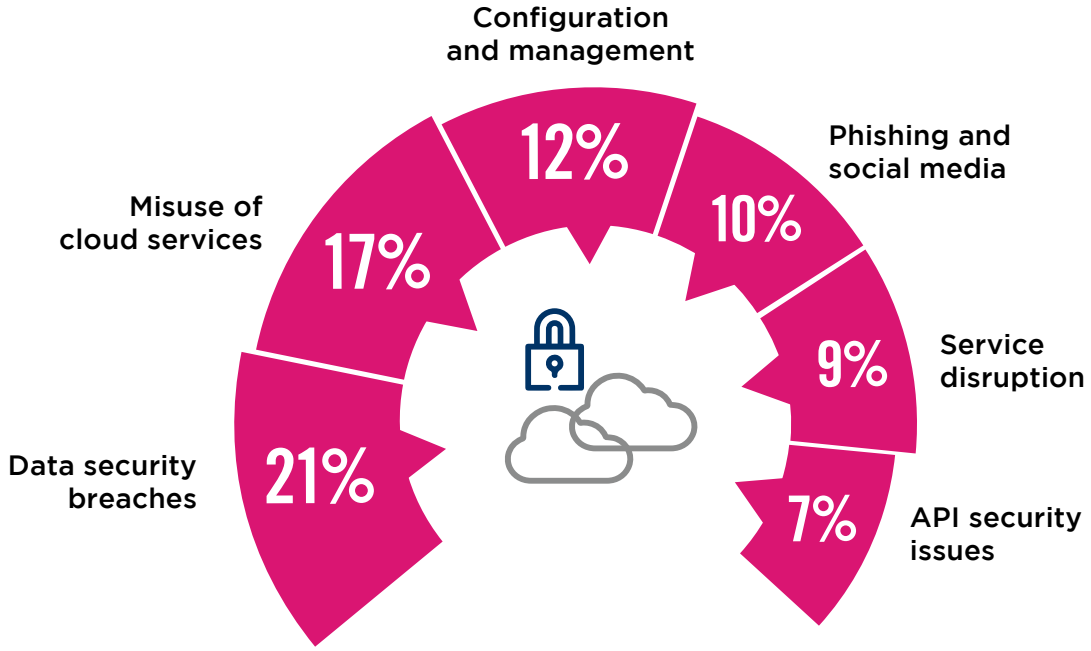
為了應對這些增加的事件和盲點，組織應採取預防為先的方法，確保採用主動而非被動安全措施。利用先進、採用人工智慧 (AI) 技術的資安解決方案，有助於在潛在威脅造成重大損害之前加以預測和減輕，進而與整個產業向更積極主動的安全策略的轉變維持一致。

最常見的雲端資安事件

針對雲端環境中遇到的特定類型事件量身打造網路安全策略，對於有效應對普遍存在的威脅至關重要，這對 2024 年及以後尤其重要。

在過去幾年中，錯誤配置一直是安全事件的主要推動因素，也是大多數組織的重點。然而，今年我們看到資料安全漏洞以 **21%** 的比例位居首位。**17%** 的受訪者指出的雲端服務濫用顯示雲端資源被大量用於惡意目的，**12%** 的受訪者報告了配置和管理錯誤，排名下降了幾位。

If your organization experienced any security incidents related to public cloud usage in the last 12 months, what type of incident occured?



其他回應包括：供應鏈攻擊 6% | 惡意軟體相關事件 5% | 使用者活動相關 3% | 合規性違規 3% 軟體脆弱性 3% | 其他 4%

重要見解：

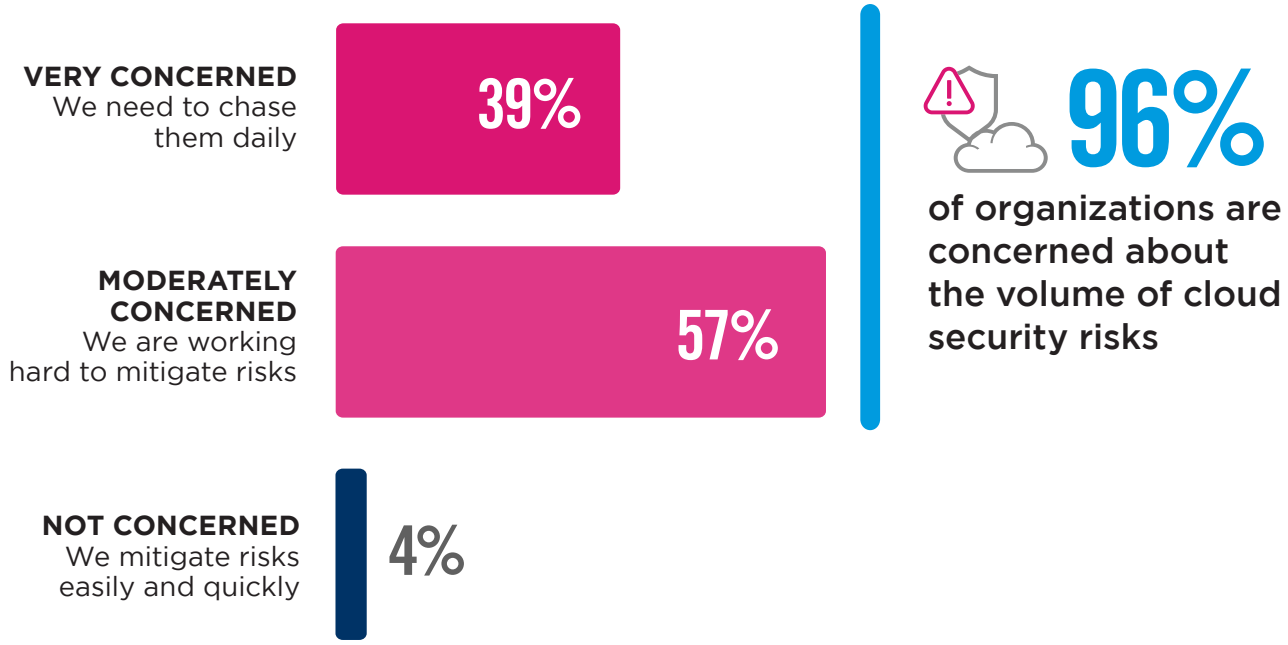
儘管雲端資安態勢管理 (CSPM) 已成為許多組織的常見安全實務，旨在確保實施適當的政策和控制以識別錯誤配置，但資料入侵事件的增加凸顯了優先保護包含敏感資料之雲端資產的必要性。新增資料安全態勢管理 (DSPM) 等安全組件可為安全團隊提供更多可見性，以了解敏感資料所在位置、誰有權存取這些資料，以及這些資料的使用方式。

雲端資安問題

了解 IT 專業人員對雲端資安風險的擔憂程度有助於評估目前安全措施的有效性。

高達 **96%** 的受訪者對他們管理這些風險的能力感到擔憂，其中 **39%** 表示非常擔憂，這凸顯出稀缺資源方面的巨大壓力，並強調對更積極主動之安全解決方案的需求。

How concerned are you with the volume of cloud security risks that require mitigation?



重要見解：

雲端持續創新和複雜化，導致雲端資安現在是由開發運營和開發人員團隊來管理和實施。隨著時間推移，許多 CISO 組織已將控制權交給開發運營，失去了可見性和監督權。

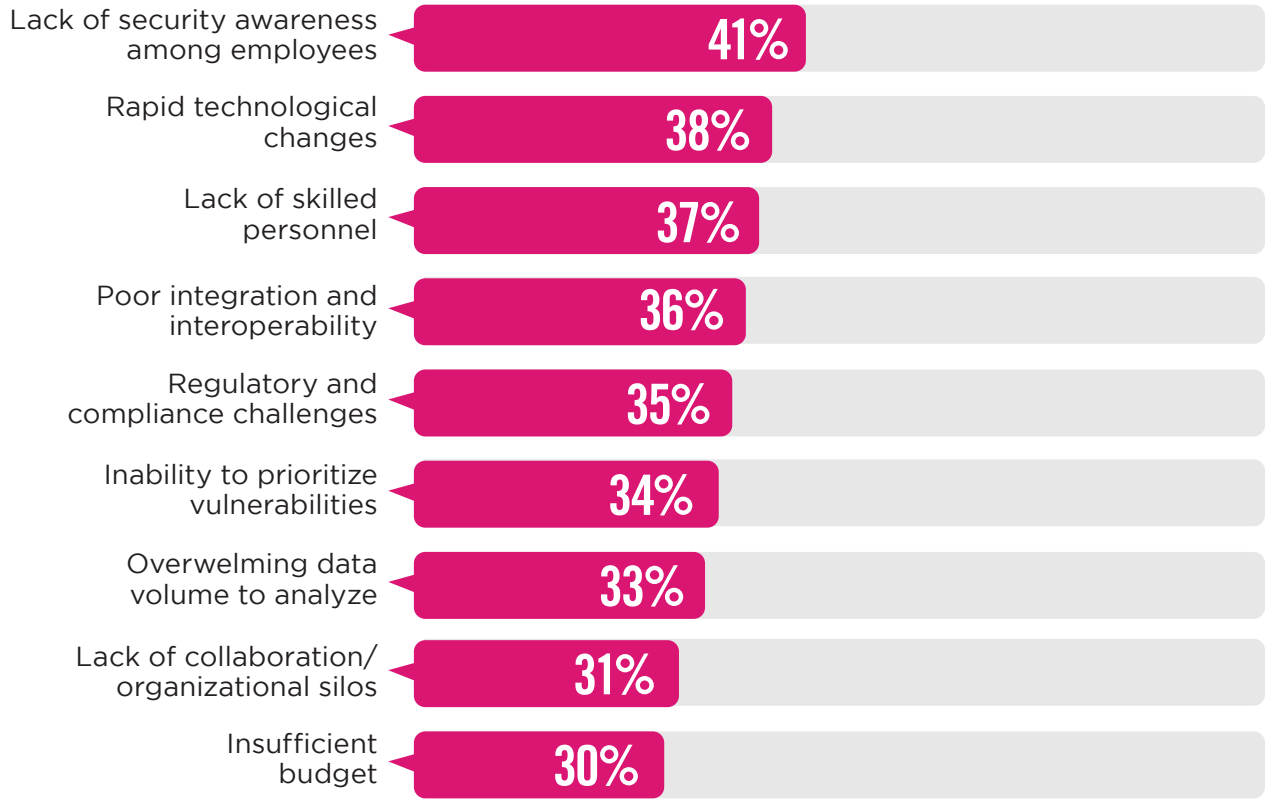
現在是時候進行典範轉移，超越傳統的偵測和修復週期，讓組織能在不將安全營運完全交由開發人員的情況下保護雲端環境。

有效網路防禦的障礙

了解組織在防禦網路威脅時所面臨的主要障礙，對於完善網路安全策略和資源分配至關重要。**41%** 的受訪者表示，最大的障礙是現有員工缺乏安全意識，這凸顯了在各個組織層級實施全面培訓計畫以加強安全知識的必要性。**38%** 和 **37%** 的受訪者分別提到了技術的快速變化和缺乏熟練人員，凸顯出在跟上不斷發展的威脅和應對這些威脅的技術方面的困難。

此外，**36%** 的參與者認為安全解決方案之間的整合和互通性差是主要挑戰，這點顯示有凝聚力的安全環境可顯著提高防禦能力。

Which of the following barriers inhibit your organization from adequately defending against cyberthreats?



其他回應包括：難以證明額外投資的合理性 29% | 安全工具的情境資訊不足 28% | 供應鏈脆弱性 26% | 缺乏管理層支持 24% | 對有效解決方案投資不足 23% | 不確定/其他 13%

重要見解：

為克服這些障礙，組織應考慮對現有員工進行進階培訓和發展，以縮小技能差距。此外，諮詢服務還能進一步協助企業跨各種工具和平台整合安全解決方案，並釋放有限資源。

網路安全人才短缺

深入探討員工資源限制問題後，我們發現組織不僅在保持最新的網路安全技能方面遇到困難，而且調查結果凸顯了許多組織在招聘新的網路安全專業人才方面面臨的挑戰，**76%** 的受訪者表示缺乏熟練的網路安全專業人員。

如此龐大的數字凸顯出業界普遍存在的問題，即對網路安全人才的需求在未來幾年內遠遠供不應求，這可能會導致關鍵安全職位人員不足，脆弱性得不到解決。

Is your organization currently facing a shortage of cybersecurity talent?

重要見解：

組織可以透過投資受管理的雲端原生應用保護平台 (CNAPP) 來彌補這些不足並發展團隊的專業知識。這種方法透過與組織的 IT 和資訊安全 (InfoSec) 營運無縫整合，以實現更好的監控、設定、政策調整、事件管理、疑難排解等，有助於彌補人員短缺並填補知識空白。

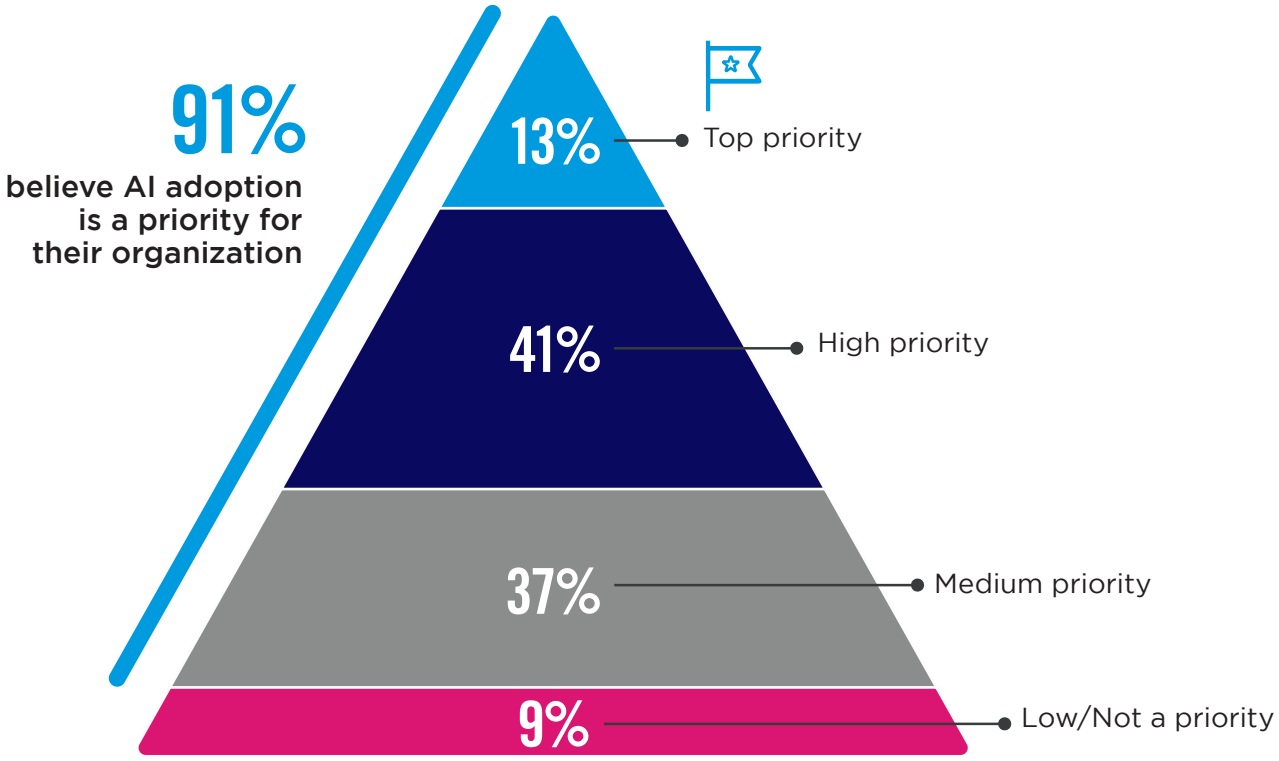
此外，整合利用人工智慧和自動化的進階安全解決方案可以彌補人力資源的短缺。這些技術能比人類團隊更有效率地執行日常安全任務並分析大量安全資料，讓現有員工能專注於更具策略性、影響更大的安全計畫。

人工智慧在網路安全中的優先地位

將人工智慧 (AI) 整合到網路安全策略中，是組織如何看待先進技術在增強安全態勢方面之作用的重要指標。

大多數受訪者 **(91%)** 將人工智慧視為首要事項，顯示他們明顯傾向在網路安全策略中採用人工智慧驅動的解決方案。這種重視凸顯出對人工智慧增強安全措施的依賴日益增加，因為人工智慧能夠快速分析大量資料、偵測異常，並以單憑人類分析師無法企及的精確度和速度預測潛在威脅。

How does AI adoption rank among your organization's cybersecurity priorities?



重要見解：

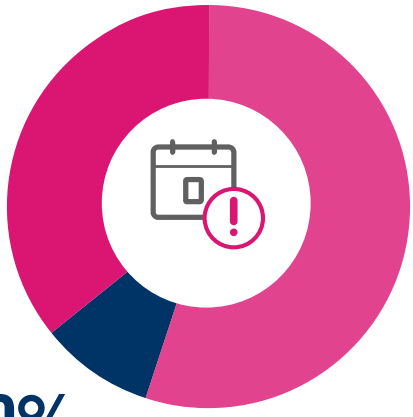
組織應考慮提升人工智慧在其網路安全策略中的作用，特別是透過利用主動式網路應用程式防火牆和進階網路安全系統等人工智慧驅動的工具。這些人工智慧增強型工具可透過不斷學習和適應新的威脅，顯著改善對複雜網路威脅的偵測和預防，尤其是零時差攻擊。

應對零時差威脅

技術的快速發展提高了網路犯罪分子發動更複雜攻擊的能力。

幾乎所有受訪者 **(91%)** 都擔心其安全系統應對零時差攻擊和未知風險的能力，這顯示目前的安全措施存在重大差距，無法在這些攻擊造成危害之前充分預防或加以緩解。

How concerned are you about unknown risks and zero-day attacks such as Log4j / Log4Shell?



36%
VERY CONCERNED
We don't believe that our security measures will be able to handle these attacks

55%
MODERATELY CONCERNED
We have the right security measures in place

9%
NOT CONCERNED
We have strong security capabilities in place that have prevented previous attacks

重要見解：

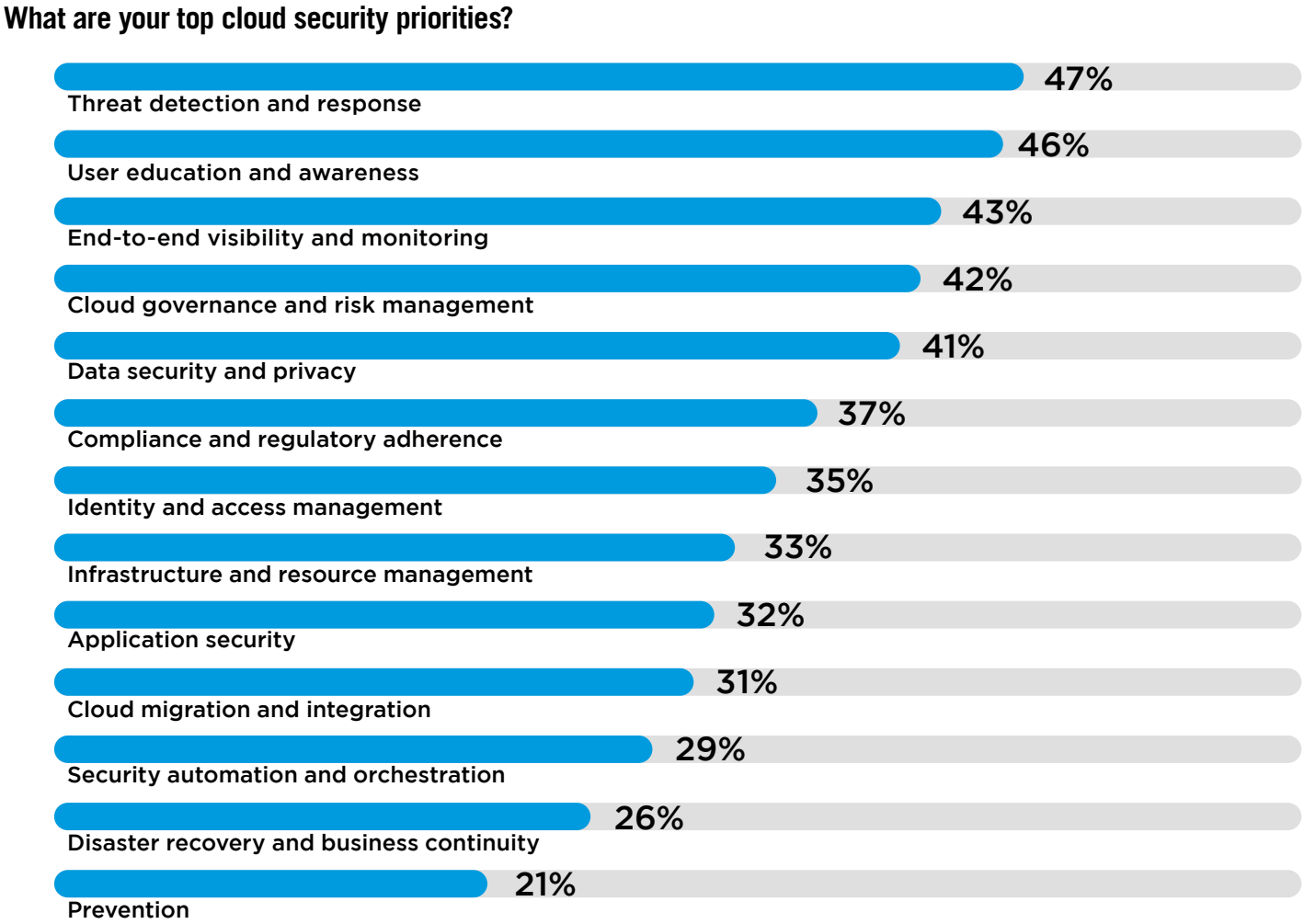
現代網頁應用程式防火牆 (WAF)，特別是利用人工智慧提供即時和預測性保護而不依賴簽名的網頁應用程式防火牆，可作為雲端「前門」的第一道關鍵防線，在惡意企圖深入滲透到網路之前加以阻止。將其與提供深度資料包偵測和跨所有存取點之即時威脅偵測的進階網路安全解決方案相結合，可大幅降低雲端環境遭受零時差攻擊的脆弱性。

這些技術在無縫安全架構中整合時，可確保強大的防禦機制，不僅能偵測還能防止攻擊，進而維持雲端基礎架構的完整性和復原能力，以應對最無法預測的威脅。

雲端資安不斷演變的首要事項

隨著組織在安全事件和資料入侵不斷增加的情況下應對雲端資安的複雜性，調查顯示，**47%** 的受訪者將威脅偵測和回應作為首要事項，重點關注此領域。這種方法反映了傳統被動的立場，即僅依靠在威脅發生時識別和緩解威脅。

有趣的是，儘管網路威脅日益複雜，但只有 **21%** 的組織優先考慮旨在阻止攻擊發生的預防策略。



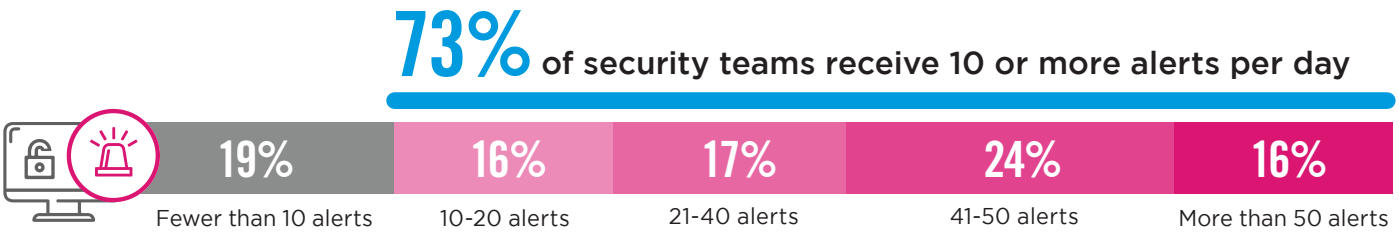
重要見解：

這種預防差距凸顯出目前安全工作中一項關鍵且常見的疏忽—雖然威脅偵測和監控必不可少，但其往往依賴於識別已知的脆弱性和惡意行為模式。這種方法在應對新型威脅時顯得不足，特別是零時差攻擊。零時差攻擊利用的是以前未知的脆弱性，因此無法使用傳統的安全工具偵測到。更均衡的策略包含強大的預防機制，透過減少對攻擊發生後才進行事後減災的依賴，以加強整體安全性。

安全反應緩慢

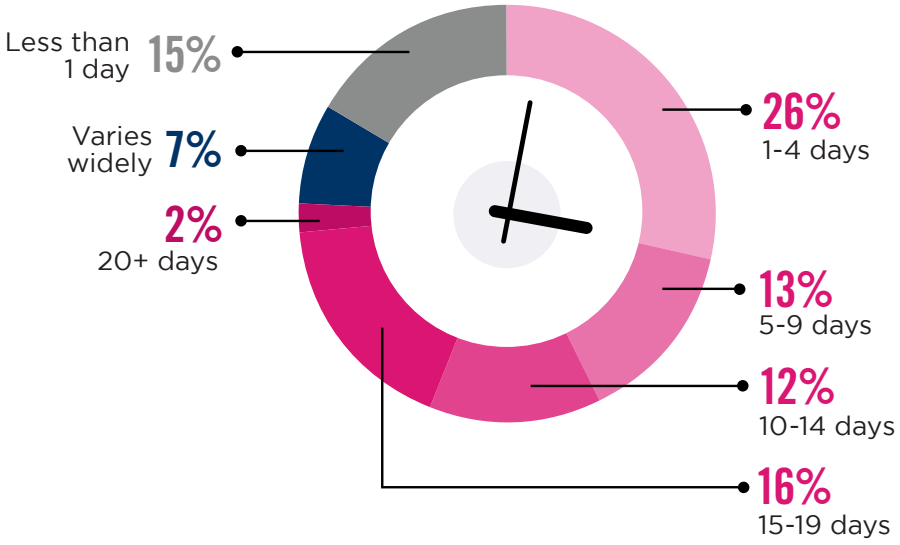
調查證實了網路安全營運面臨的最大挑戰之一：每天大量的安全警報。值得注意的是，**40%** 的組織每天收到超過 40 個警報。這種情況不僅耗費了資安監控中心 (SOC) 分析師的資源，而且還延長了解決每個警報所需的時間，**43%** 的組織回報解決時間超過五天。這種警報氾濫會讓團隊疲於奔命，並因延遲應對潛在的關鍵威脅而增加脆弱性。

How many security alerts does your security team receive on an average day?



不確定 8%

How long does it typically take your team to resolve a security issue?



67% take between 1 and 19 days to resolve a security issue

不確定 9%

重要見解：

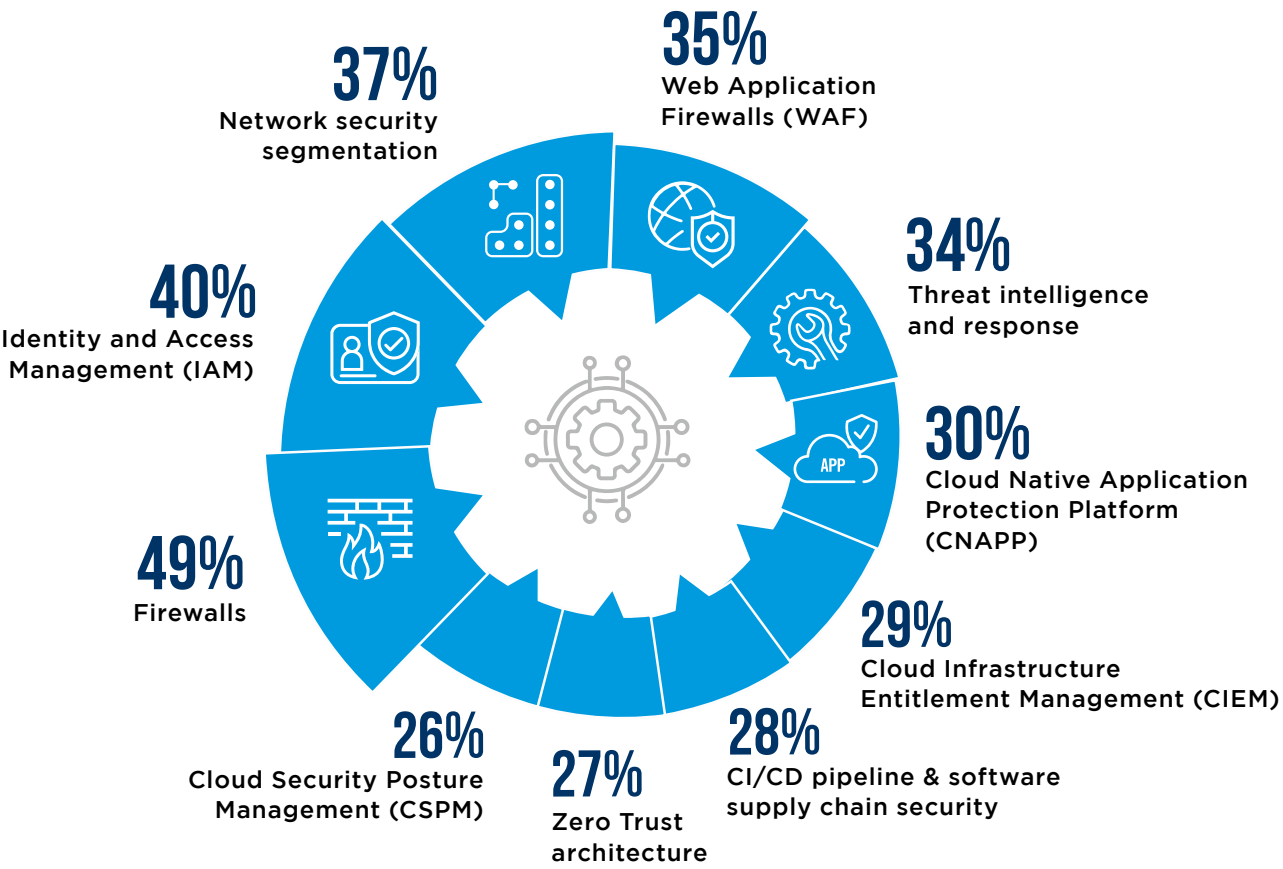
組織在掃描其雲端環境時發現數百萬個潛在問題是很常見的—除非惡意行為者能夠利用這些問題，否則大多數問題是無害的。為了應對此挑戰，供應商已實施「攻擊圖」，對靜態錯誤配置和脆弱性進行分組和關聯，以更清楚確定警報的優先順序。然而，確定優先順序是不夠的，因為團隊可能仍然會忽略低於關注閾值的警報。這種虛假的安全感可能會產生不利影響。透過專注於在攻擊發生之前就加以預防，組織可以顯著減少原本會被視為高風險的警報數量。這種轉變不僅可以釋放寶貴的資源，還可以增強組織徹底調查和管理原本會構成重大威脅的真正風險的能力。

應對網路安全工具碎片化

調查顯示，組織用於管理其雲端基礎架構的安全平台和工具存在嚴重的碎片化。防火牆作為主要的防禦措施 **(49%)**，反映出其在網路安全中的關鍵作用。然而，只有 **37%** 的組織有效實施分段策略。這種疏忽可能特別有害，因為分段不足會讓攻擊者利用脆弱性，進而獲得對網路更廣泛部分的存取權，造成廣泛的損害。

有 **35%** 的受訪者使用網頁應用程式防火牆，**26%** 的受訪者使用雲端資安態勢管理 (CSPM)，這顯示安全採用分層方法，既能解決網路防禦問題，又能解決應用程式層面的脆弱性，以及介於兩者之間的所有問題。

What are your organization's primary measures and controls to manage your entire cloud infrastructure?



其他回應包括：Kubernetes 安全態勢管理 (KSPM) 26% | 雲端工作負載保護平台 (CWPP) 25% | 內容撤防與重建 (CDR) 12%

雲端政策蔓延

雖然我們看到對各種雲端安全組件的理解和利用顯著增加，但越來越多的安全解決方案 (**43%** 的企業使用七種或七種以上的工具來配置政策就凸顯了此點) 顯示安全環境複雜且效率低下。

How many separate security solutions are required to configure the policies securing your enterprise's entire cloud footprint?

83%

have to access 4 or more dashboards to configure their enterprise's cloud policies

重要見解：

將安全措施整合到一個高度整合的平台中，無需多個互不關聯的工具即可提供全面覆蓋，才是未來的發展方向。

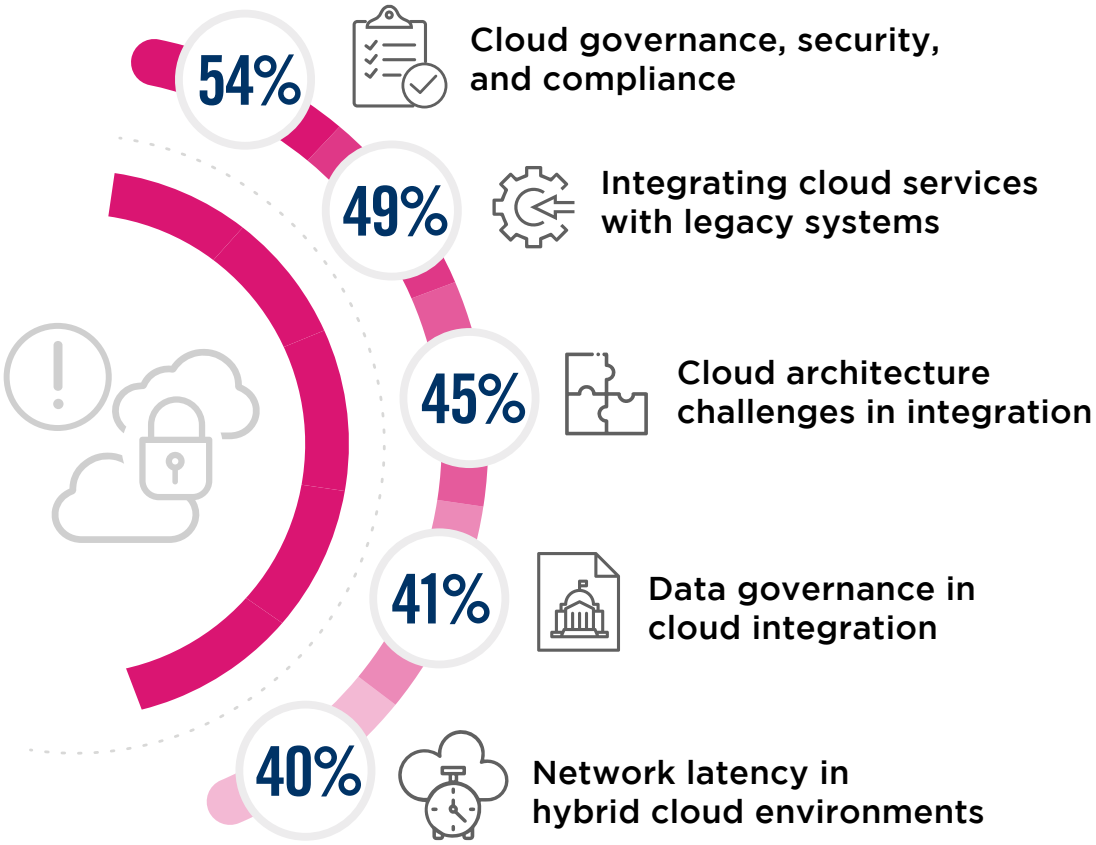
透過將網頁應用程式防火牆、網路分段、雲端偵測和回應，以及雲端原生應用程式防護平台等更廣泛的功能整合到一個保護傘下，企業可以在簡化管理負擔的同時提高安全效能。

雲端整合挑戰

如果組織面臨的大多數安全問題都能透過更精簡的解決方案來緩解，為什麼工具和政策的數量每年都在繼續增加？本調查揭示了組織在嘗試更有效整合雲端資安時所面臨的痛苦。

在混合雲端或多雲端架構中維護一致監管標準的複雜性變得顯而易見，因為 **54%** 的受訪者努力確保跨不同環境的合規和雲端治理。此外，將近一半 **(49%)** 的受訪者在將雲端服務整合到老化的傳統系統方面遇到困難，而稀缺的 IT 資源可能會妨礙有效和安全的整合，讓這項任務變得更複雜。

What cloud integration challenges do you face?

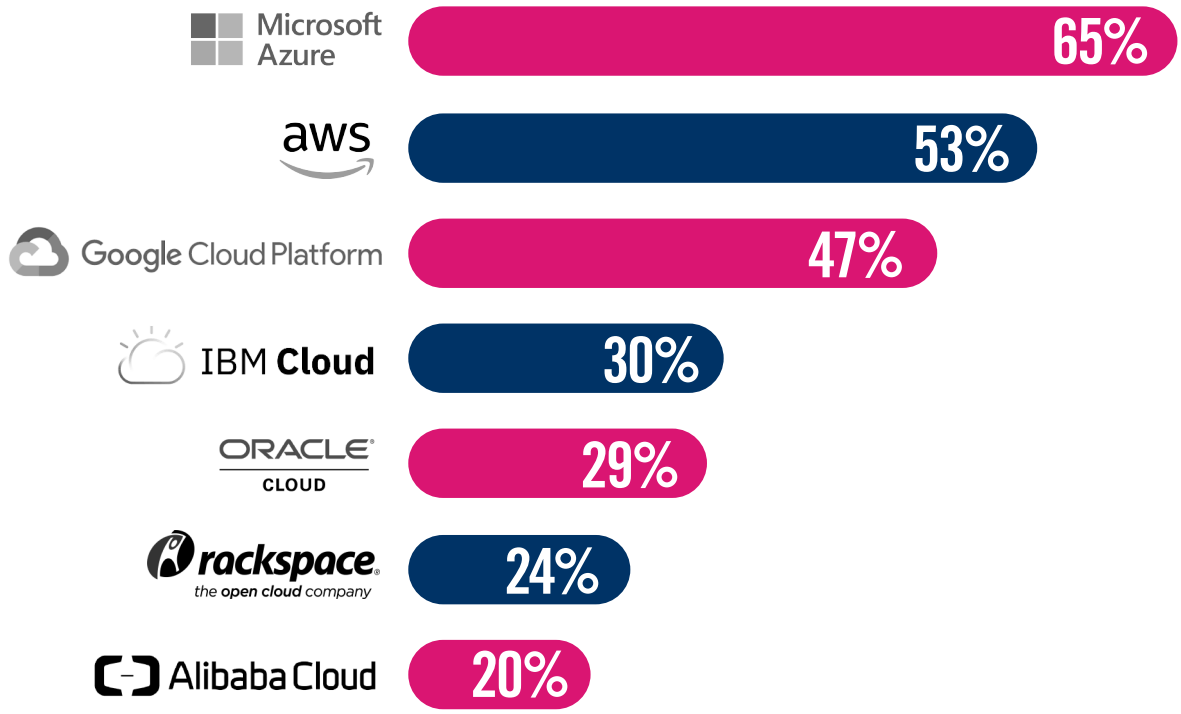


其他回應包括：在自訂和預先建置整合之間做出決定 39% | 由雲端整合反模式引起的問題 29% 供應商鎖定問題 27%

雲端服務的供應商

談到整合挑戰時，必須注意的是，大多數組織也在其安全環境中管理多個雲端基礎架構式服務提供商。調查顯示，Microsoft Azure 在市場上處於領先地位，**65%** 的受訪者部署其雲端服務，其次是 Amazon Web Services (AWS) (**53%**) 和 Google Cloud (**47%**)。

What cloud IaaS provider(s) do you currently use or plan to use in the future?



重要見解：

雲端原生解決方案通常在雲端服務 (包括內部部署資料中心) 之間缺乏統一性，導致不同的政策並使安全監督複雜化。尋找與各種雲端資安提供商的廣域網路基礎架構緊密整合的網路安全解決方案，以便在不同的雲端環境中普遍套用規則。

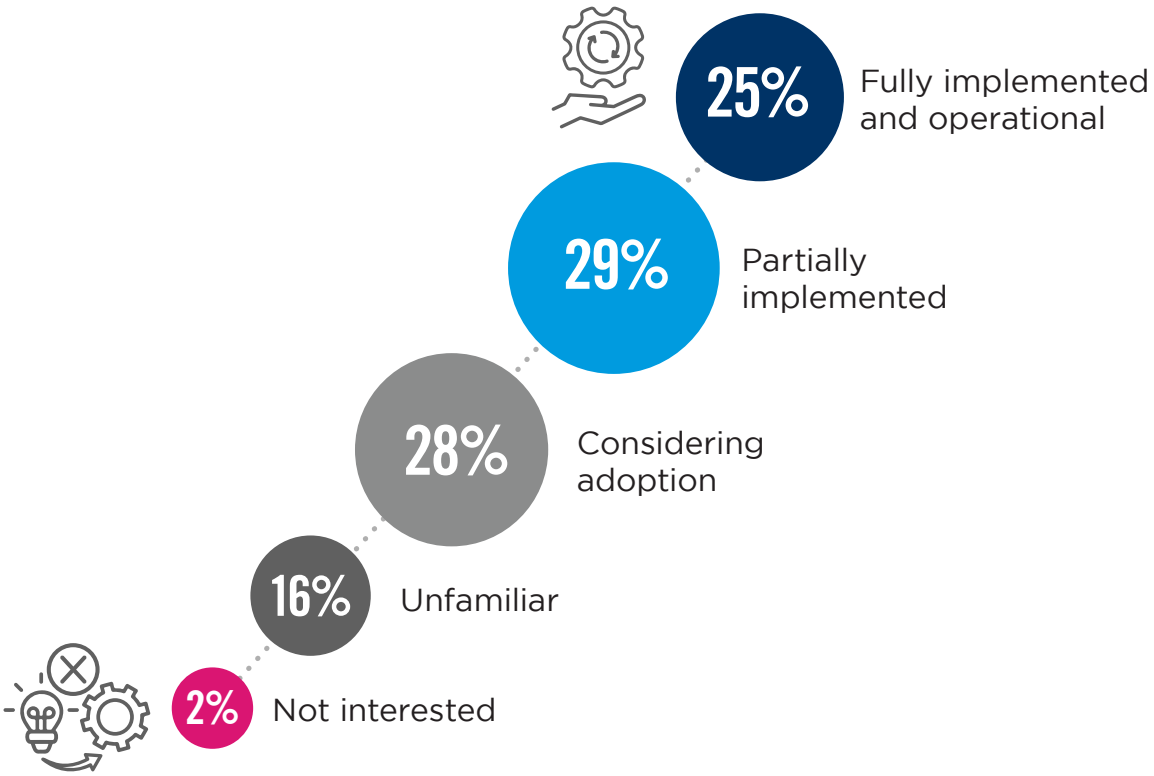
透過將網頁應用程式防火牆作為服務與應用程式開發介面模式發現相結合，組織能夠進一步簡化內部部署流程。領先的供應商在雲端原生應用程式防護平台中提供這種層級的進階安全性，以確保易於整合和全面覆蓋。

快速雲端原生應用程式防護平台 + 預防採用

雲端原生應用程式防護平台應成為任何雲端資安策略的基石，因其統一了雲端資安態勢管理 (CSPM)、雲端工作負載保護 (CWP)、雲端基礎架構授權管理 (CIEM)、雲端偵測和回應 (CDR) 以及程式碼安全性，使其更容易實現流程自動化並減少人工低效率。

調查顯示，採用雲端原生應用程式防護平台的趨勢令人鼓舞：**25%** 的組織已全面實施雲端原生應用程式防護平台解決方案，這顯示組織對進階雲端資安實務的堅定承諾。另有 **29%** 的組織正在將雲端原生應用程式防護平台整合到其系統中，這顯示大多數受訪者認識到了此類平台的優勢。

What is your organization's current stage of CNAPP (Cloud Native Application Protection Platform) adoption?



重要見解：

並非所有雲端原生應用程式防護平台都是一樣的。請確保您投資的平台能提供只有透過整合網頁應用程式防火牆和網路安全才能找到的預防性元件。市面上的大多數解決方案都忽略了這個重要的整合，因此會產生過多警報和風險因素。

利用更多強調預防而非修復的元件來增強雲端原生應用程式防護平台系統，可以強化雲端基礎架構。

主動雲端防禦策略

隨著雲端威脅變得越來越頻繁和複雜，組織必須利用以下雲端資安架構，從傳統的被動安全措施轉變為預防為先的方法。

採用人工智慧支援的網頁應用程式防火牆進行零時差保護：
由於 91% 的受訪者擔心零時差攻擊，因此採用人工智慧支援的網路應用程式防火牆至關重要。這些網路應用程式防火牆可智慧地應對網路威脅，包括零時差漏洞利用，而無需依賴於基於簽名的偵測，提供與現代攻擊媒介一致的即時保護。

部署進階網路安全：
考慮採用可與雲端基礎架構一起擴展的進階網路安全解決方案。此解決方案應支援無縫整合並提供全面保護，促進宏觀和微觀分段及跨雲端平台的統一政策管理。

採用預防為先的方法：
由於對威脅偵測的關注度很高 (47%)，採用預防為先的雲端原生應用程式防護平台能將方法從被動轉為主動。此平台可將警報次數降至最低，並納入預防措施，可顯著減少稀缺的安全分析師需要注意的風險數量。

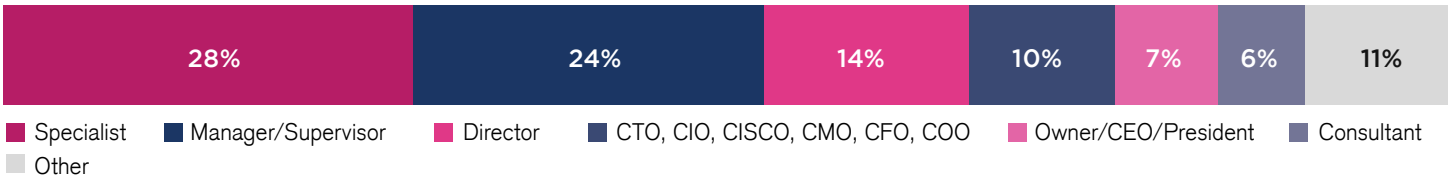
利用全面的雲端原生應用程式防護平台功能：
43% 的受訪者使用七種或七種以上的工具來設定政策，這凸顯了管理的複雜性，因此應採用具有雲端工作負載保護、雲端偵測和回應、程式碼安全和雲端資安態勢管理等豐富功能的進階雲端原生應用程式防護平台。這些功能有助於簡化安全流程，並加強對雲端環境的管理。

整合人工智慧技術：
隨著 91% 的組織現在優先考慮人工智慧來增強其安全態勢，重點已轉向利用人工智慧進行主動威脅預防和加強員工不足。

方法論和人口統計

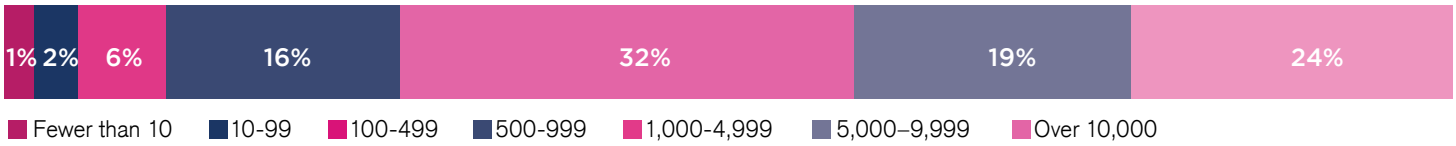
《2024 年雲端資安報告》是根據 2024 年 4 月對 813 名網路安全專業人員進行的深入調查。這項研究提供了雲端資安管理方面的見解和趨勢，凸顯出組織面臨的威脅和迫切挑戰，同時為加強雲端資安態勢提供指導。參與者涵蓋各種職務，從技術和業務主管到實際動手操作的 IT 安全從業人員，代表了不同規模和產業的組織均衡組合。

CAREER LEVEL

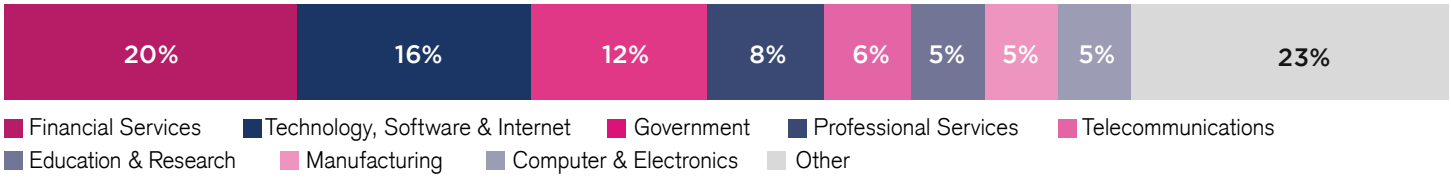


DEPARTMENT

COMPANY SIZE



INDUSTRY



Check Point Software Technologies Ltd. 是領先的人工智慧驅動雲端資安平台供應商，為全球超過 10 萬家組織提供防護。Check Point 善用無處不在的人工智慧的力量，透過 Infinity 平台提升資安效率與準確度，其業界領先的攔截率能主動預測威脅，並縮短反應時間。此全方位平台包含多種雲端交付技術，包括保護工作空間的 Check Point Harmony、保護雲端的 Check Point CloudGuard、保護網路的 Check Point Quantum，以及提供協作資安作業與服務的 Check Point Infinity 核心服務。

www.checkpoint.com

Cybersecurity INSIDERS

Cybersecurity Insiders 匯聚超過 60 萬名 IT 安全專業人士與世界一流的技術供應商，以促進智慧解決方案的制定及協作，共同解決當今最關鍵的資安挑戰。

我們的方法專注於建立和策劃獨特的內容，教育並告知網路安全專業人員最新的網路安全趨勢、解決方案和最佳實務。從全面的研究報告和公正的產品評論到實用的電子指南、引人入勝的網路研討會和教育文章，我們致力於提供資源，為當今複雜的網路安全挑戰提供基於證據的答案。

立即聯絡我們，了解 Cybersecurity Insiders 如何協助您在擁擠的市場中脫穎而出，並提高需求、品牌知名度和思想領導力。

請寄電子郵件至 info@cybersecurity-insiders.com 或造訪 cybersecurity-insiders.com