SURVIVAL

Guide to Security

IBM Security

IBM Security

面對威脅，你該採取的關鍵五術

資料外洩所帶來的企業成本逐年偏高，每年資料被外洩的消費者數量也越來越多，
平均每次資料外洩事件會為企業造成 392 萬美金的成本損失；而每筆資料外洩的成本約為 150 美金，
企業平均從找出資料外洩的根本原因到將外洩問題獲得妥善控制需要花上 279 天！
惡意攻擊已經成為資料外洩事件的最重要原因，有 51% 的資料外洩都源自於攻擊行動，
系統故障占了 25%，人為疏失占 24%。

台灣因為資安威脅造成的損失即高達新台幣 8100 億元，幾乎等同全台灣 5% GDP。
更別說是重要基礎建設，像是連網的醫療設備、無人機、無人車等遭受到惡意攻擊，
危害的就不只是金錢或競爭力，而是直接衝擊我們的生命安全。

2018 年 知名半導體公司全臺產線大當機，營收損失預估更是高達 52 億元天價，創下臺灣有史以來損失金額最高的資安事件
2019 年 Facebook 近四億兩千萬筆用戶個資外洩，超大型資料庫被駭客攻擊公開在網路上任意存取
2019 年 新發現 Android 木馬，不但大量竊取用戶個資，還會暗中訂閱付費服務、製造假點擊破壞廣告分潤

2020 年，你也正身處於危險之中 .....

- 憑證保護不斷被盜取：2019 年違反了 85 億條記錄，使攻擊者可以獲取更多被盜憑證
- 修補不完的資安漏洞：修補漏洞迄今為止，已發現 150,000 個漏洞
- 勒索軟體不斷更新：勒索軟體攻擊在 2019 年第四季度同比增長 67%
- 威脅者投向攻擊：媒介營運技術包含物聯網，OT 和相連的工業和醫療系統攻擊同比激增 2,000%
- 利用時下焦點話題釣魚：駭客利用大眾對於新冠肺炎的恐懼心理，製造各式偽裝成官方感染數據或衛教資訊的惡意檔案，發動網釣攻擊

Key Point **1**

IBM QRadar Security Intelligence Platform

以 SIEM 為核心，提供日誌管理、網路流量活動監控等功能，內建 IBM X-Force 全球安全威脅情資，也可輕鬆結合各大 ISAC 情資，並以 AI 為基礎提供使用者行為分析，讓資安人員能快速獲取必要的可視性，從而協助保護企業自身網路安全與 IT 資產，滿足當前資安挑戰與法規遵循要求。

連續十一年榮獲 Gartner Magic Quadrant for SIEM 魔力象限領導者殊榮

企業組織每天平均發現 200,000 起資安事件

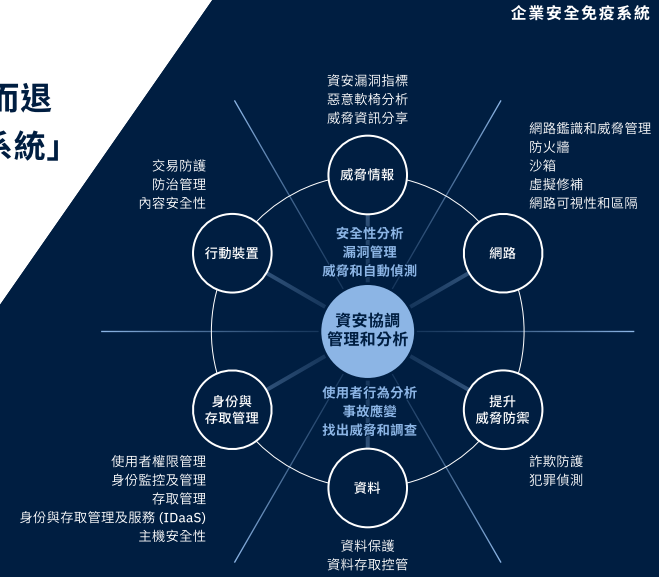
而網路犯罪被發現之前，平均潛伏期達 191 天

在這過程中你該做些什麼？

「治」不如「防」，在受到攻擊後
守住關鍵資料、流程與客戶體驗，毫髮無傷全身而退
立即打造最新一代資訊安全平台「企業安全免疫系統」

IBM QRadar 獨特之處

- AI 感知並偵測詐騙、內鬼和進階威脅
- 立即將事件正規化並產生相互關聯
- 感知、追蹤並連結重大事件和威脅
- 強制執行資料隱私原則
- 從 IBM X-Force 提供專業即時威脅情報
- 搭配 Data Store 授權提供日誌無限量儲存
- 能在本地或雲端環境中部署 QRadar SIEM



持續大量蒐集

解讀安全數據

將 Log 記錄檔與網路流量數據標準化與一致化，以供更精準深入的分析。

異常行為監測

歸納資產、使用者、服務與網路活動的行為基準，建立常態模型，用以精準監測異常行為。

偵測與分析

人工智慧運用

運用 AI 來協助安全分析師調查外在威脅事件。

行為模式分析

即時分析資安事件特徵，比對已知惡意威脅模式，快速辨識與分類資安威脅。

歷史資料分析

當攻擊者採取異常步驟來侵入系統，系統可即時偵測到這些非預期行為並立即預警。

使用者行為分析 (UBA)

持續分析個別使用者行為，偵測偏差行為，為每個企業內部使用者生成各自詳細的風險評分，並及時找出被入侵的使用者或有惡意的內鬼。

預測分析

運用行為預測模型，提前預測並偵測未來可能發生的異常行為。

使用者分群監測

依據相同的使用行為將使用者分群，持續監測每個分群中的異常行為，可更快速、更精準地辨識 風險與找到惡意使用者。

設備行為偵測

持續監控實體設備，掌握非常規行為、服務與連線，當系統被入侵時可更快察覺並介入。

統計分析

透過統計數據察覺潛伏的威脅，例如有終端設備異常送出大量資料給未授權的雲端服務等。

掌握最新資安情報

交叉比對事件特徵與資安威脅情報，例如惡意網域與雜湊值 (Hashes)。當遭受到最新型態攻 擊時可快速察覺與應變。

即時預警

整合分析結果、串聯相關資訊，建立從端到端的資安事件關聯鏈，判斷其嚴重性，並即時、自動發布警報。

事件調查

運用自然語言處理技術自動建立知識圖表，推理事件根因，提供攻擊的概觀，並且分辨相關的入侵指標。

使用 MITRE ATT&CK 加快回應及視覺化各個攻擊階段。

有最大風險的調查優先順序清單。

IBM QRadar 智慧安全分析平台 5 大助力

家賊難防，交給 IBM QRadar UBA ！

相信每一位資安專家都會同意：「人，是資安防禦最不可控的環節。」IBM QRadar 使用者行為分析 (UBA) 能夠即時分析內部人員的使用行為與活動模式，及早發現可疑的異常行為，並判斷其風險。QRadar 具備智慧分析能力，協助資安管理者將龐大使用者資料去蕪存菁，發掘異常行為、橫向移動、惡意威脅與資料竊取等潛在風險，及時預警與資安儀表板。管理者可快速鎖定使用者進行調查，提早因應防範未然。

IBM QRadar Incident Forensics 資安事件鑑定只要短短幾分鐘

系統遭到攻擊，當務之急就是還原過程、鑑定原因、修補問題。鑑識所需時間越長，暴露風險就越大。多數企業需要費時數天才能完成鑑識，早已無法因應瞬息萬變的資安賽局！ IBM QRadar Incident Forensics 可幫助您追蹤潛在攻擊者的逐步動作，快速進行惡意資安事件的深度鑒定調查，鑑識時間由數天縮短為數分鐘，並協助您重新修補安全漏洞，避免再次遭受攻擊。

讓 IBM QRadar Network Insights 大幅減輕看不完的日誌恐懼

每天收到爆滿的資安日誌 (log)，明知道惡意風險的蹤跡就藏在其中，卻無法解讀！ IBM QRadar Network Insights 正如其名：這是個網路威脅的偵測雷達，能夠即時分析網路流量與日誌數據，將隱藏的威脅攤在陽光下！ IBM QRadar Network Insights 可快速執行深度鑑定，將資安事件調查時間從數天縮短為數分鐘，大幅減少團隊調查威脅所需的的時間與心力。並協助修補網路安全漏洞，預防災難再次發生。

IBM QRadar Vulnerability Manager 幫您秒補資安漏洞

IT 環境越複雜，來自軟硬體的漏洞及其暴露的資安弱點就越令人防不勝防。IBM QRadar Vulnerability Manager 可以掃描完整網路環境，自動偵測超過 7 萬個已知風險，並結合外部資訊隨時更新，制定優先因應方案，搶在攻擊發生前就阻絕外患。

IBM QRadar Advisor with Watson 用 AI 戰勝 AI

人工智慧 (AI) 被網路犯罪份子用於攻擊行動的案例，在國際上已時有所聞。AI 不僅讓網路攻擊加速、自動化，更可模仿自然行為，達到更廣泛的社交工程與網路釣魚目的。聽起來很可怕？好消息是，您也能用 AI 來戰勝 AI ！ IBM QRadar Advisor with Watson 是 AI 界的資安專家，遍讀全球無數資安報告、新聞、研究，並建立完整「知識圖譜」(Knowledge Graph)，能快速分析非結構化資料，並建立安全攻擊的關聯性，輔助資安人員全天候 7x24 預測攻擊、即時回應！

IBM QRadar
Security Intelligence Platform

精選案例

Wimbledon 溫布頓網球錦標賽

溫布頓與 IBM Security 合作來保護其數位化活動
防止在此著名體育賽事期間遭到數以萬計的網路攻擊

業務挑戰

溫布頓數位體驗吸引了一批全新的「數位原生」觀眾，有助於提升溫布頓品牌價值；然而也面臨網路攻擊所帶來的風險。他們需要找到可信賴的資安解決方案，迅速有效地在賽事期間找出並應對近兩億事件中隱藏的即時威脅。

導入成果

速度提升 60 倍 ► Watson AI 與手動分析的安全性威脅偵測效果比較

數量增加 5 倍 ► 賽事期間能分析的資安事件量

零事故 ► 賽事沒有發生任何影響官網與其商譽的資料外洩

客戶推薦

Alexandra Willis 表示：「雖然我們花了一年時間在籌備溫布頓，但我們必須在兩週期間呈現完美賽事，尤其是我們要面對數以千萬計球迷。」「如果兩週賽事期間發生資安事故將會重擊溫布頓的商譽。溫布頓是英國人民引以為傲的賽事，若不肖份子趁機作亂則不只是影響一場網球賽事而已。」我們必須「固若金湯」。IBM 首席工程師與歐洲區技術長 Martin Borrett 表示：「賽事期間我們偵測到近 2 億起資安事件。溫布頓信賴 IBM Security 與我們的雲端服務能偵測並阻擋即時威脅。」溫布頓官網受到數個安全性產品的保護，其核心產品係採用 IBM QRadar SIEM 安全情報平台，其能匯集不同基礎架構中數千個端點與裝置的資料，並分析其關聯性以協助安全性團隊判斷事件的輕重緩急並找出所面對的威脅。


IBM QRadar
Security Intelligence Platform

IBM QRadar Security Intelligence Platform

立即免費試用

或撥打 0800-016-888 按 1
立即聯絡 IBM 業務代表提供進一步協助

Key Point **2**

IBM X-Force Exchange

即時識別全球惡意威脅情報的雲端共享平台，直接與防火牆、入侵防禦系統及 SIEM 進行整合，提供潛在風險最佳行動指示，永遠領先新興威脅攻擊一步。

IBM X-Force Exchange

全球觀測、預警辨識、搶先扼止讓防護一步到位

即時存取豐富的威脅情報資料

IBM X-Force Exchange 提供的開放式平台能增加入侵指標 (IOC) 的環境定義，並結合智能產生的洞察分析。提供即時威脅情報，並且每分鐘動態更新一次。軟體監控超過 250 億個網頁是否有 Web 威脅，並超過 96,000 個漏洞分析資料庫作為支援。其中提供數百萬垃圾郵件和網路釣魚攻擊的深度情報，並監控含有惡意 IP 位址的聲譽資料。

共用威脅情報的協作平台

您可以與同行交流，確認研究發現，共用入侵指標的收集內容，幫助彼此做好鑑定調查，或透過私人團隊和共用群組，與同儕協作加速威脅環境的分析。

整合式解決方案有助於快速扼止威脅

此解決方案專為第三方整合而設計，擁有 Structured Threat Information Expression (STIX) 和 Trusted Automated Exchange of Indicator Information (TAXII) 的支援，這些都是自動威脅情報分享的既有標準。這能讓 IBM Security 產品與 X-Force Exchange 來源的行動情報相整合。應用程式設計介面 (API) 可讓您將威脅情報連結到自身的安全產品工具。

簡單直觀的介面，群組共享討論

一旦產生報告，使用者便能增加註解，為其他使用者提供額外的洞察和環境定義，或將報告加到群組中。使用者也可以提供意見給 X-Force 團隊，讓他們執行特定報告的分析，進而能更新內容。設定自訂通知和觀察名單，讓使用者收到感興趣領域的相關建議。

透過觀察名單來監控適用指標

只要維護一份待監控的關鍵字或產品名單，就能研究入侵指標、執行安全調查，然後觀察基礎架構中目標技術上的漏洞。如果漏洞符合觀察名單上的關鍵字或產品，您就會自動收到通知。若要對這些漏洞採取行動，您可以將漏洞加到群組中，並透過 API 或使用 STIX/TAXII 通訊協定匯入至 SIEM。

將第三方威脅情報授權加到平台

X-Force Exchange 中的 Threat Feed Manager 能從多個來源取出資料，並匯整成一個檢視，過程輕鬆簡單。您可以為供應商提供認證，直接在平台上啟用第三方威脅情報來源，這樣平台就會直接將資料整合至 X-Force Exchange。

從 IBM X-Force 取得最新的行動威脅情報

IBM X-Force 研究團隊會透過公開的群組，針對惡意軟體活動和新威脅持續增加新的情報。這些群組由 X-Force 安全專家統籌，會在平台上將人工環境定義加到入侵指標中。詳細資料包含 TLP 評分、時間範圍、目標地區、活動詳情，以及深入瞭解相關參考的連結。當有新資訊可用時，使用者可以依照集合通知更新。

如何使用 X-Force Exchange，減輕您的資安防線負擔？

透過瞭解攻擊者的意圖，例如無差別攻擊或是目標式攻擊，分析各項指標
得到具體場景脈絡的高階威脅情資，並立刻建議因應行動，協助企業管理者做出關鍵決策。

即時搜尋最新威脅

X-Force Exchange 監控超過 250 億個網頁是否有 Web 威脅，並由超過 96,000 個漏洞的資料庫作為支援。讓您能即時搜尋與追蹤最新威脅情報。

全球資安專家共享協作

全球使用者在 X-Force Exchange 上可透過公開或私密群組共享研究、驗證威脅與研議攻擊回應計畫。

高度整合串接應用

提供 API 讓您無縫整合各式安全相關應用，包括支援開放式的標準環境。更容易的將威脅預警直接串接使用。

IBM X-Force Exchange

精選案例

美國城市安全團隊
有效減少 40% 的時間處理潛在攻擊

美國城市安全中心與 IBM X-Force Exchange 合作
成功預防數百萬個潛在網站攻擊，並有效分流威脅攻擊

業務挑戰

美國城市安全中心隊經常面對微小零星但大量的網站攻擊與潛在威脅，與 IBM 攜手打造 IT 數位化基礎建置，在一個月內，阻止數百萬個微小威脅攻擊事件。其中，有效分流讓極少數的攻擊，被判斷為需要進一步調查，而這些威脅可能會影響到相關的資安團隊運作效率。

導入成果

減少 40% 威脅處理時間 ► 解決威脅問題，在時間與成本上有效減少 40% 以上的時間成本。

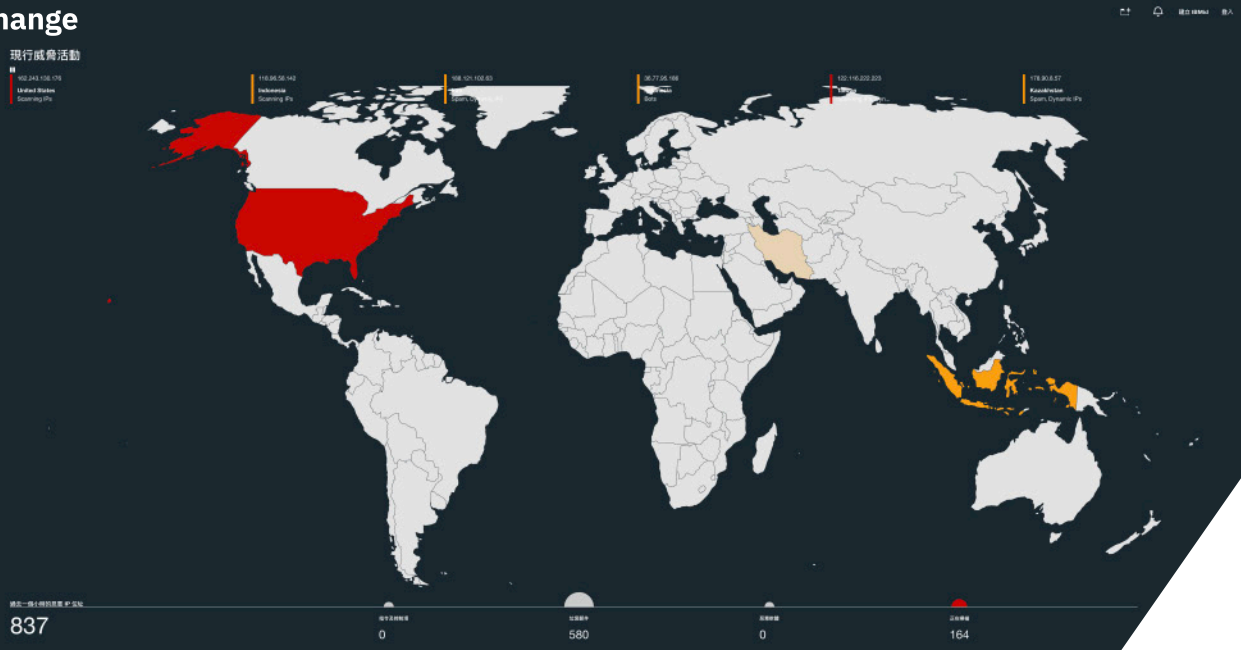
減少 18% 管理時間 ► 有效減少人員在安全風險管理上的時間，提高管理控管效率。

人力成本節省 50% ► 提高資訊安全團隊的效率，幫助其節省了 50% 的人力成本。

客戶推薦

IBM 幫助該市部署了複雜的智能資安解決方案，本解決方案集結成安全訊息和事件管理 (SIEM)，日誌管理，異常檢測和配置及漏洞管理的辦法，阻止最嚴重的安全事件。本解決方案集中並分析對數十個不同系統的監視，已從網路上發生數百個可疑事件中，分辨出優先處理的資安事件。

IBM X-Force Exchange



IBM X-Force Exchange

立即免費試用

或撥打 0800-016-888 按 1
立即聯絡 IBM 業務代表提供進一步協助

Key Point **3**

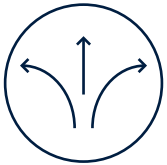
IBM Cloud Identity

運用雲端單一登入 (SSO)、多因子認證和身分識別控管來有效保護您的企業內部系統。並提供熱門 SaaS 應用程式存取、並預先建置多種範本以協助整合企業內部應用程式。為現今企業遠程辦公的最佳利器，免去使用 VPN 高授權費用與頻寬滿載問題！

IBM Cloud Identity 三大措施防護到位

所有裝置單一登入 (SSO)

提供統一的應用程式啟動程式和 SSO，以便從任何裝置都能單一登入任何應用程式。



使用 2FA 登入任何企業系統

使用彈性的 MFA 來保護 Web、雲端、行動、VPN 及作業系統。

監測管理雲端使用

要求、核准、供應與重新認證使用者的應用程式存取。透過風險評分、法規遵循資料及 URL 位置來評估並瞭解雲端應用程式風險。

以單一登入方式進行登入

免除輸入使用者名稱和密碼的麻煩。運用一組登入認證即可登入所有應用程式，讓您一鍵存取瀏覽器、行動裝置及內部部署應用程式。

透過連接器輕鬆連接 1000 多種應用程式

透過預先建置的連接器或一般範本來加快公司採用新的應用程式。

運用多因子鑑別來強化安全

利用自訂鑑別原則來加強安全並符合法令規定。使用 IBM Verify 來注入多種使用者鑑別方法以強化安全。

透過使用者自我管理選項來縮減 IT Helpdesk 人力

提供使用者自我管理介面，讓員工可以要求存取應用程式，並且重設與管理自己的密碼。

執行重新認證活動

安排定期的存取檢討，以確保持續合規。

利用 IBM MaaS360 Integration 將 SSO 延伸到企業應用程式

將 SSO 無縫延伸到企業行動性管理解決方案所涵蓋的應用程式。

利用應用程式啟動程式輕鬆尋找應用程式

從集中位置便利地尋找、檢視與存取您所有的應用程式。啟動程式會整合所有應用程式，包括內部部署和雲端中的應用程式。

將 MFA 內嵌至消費者或面對民眾的應用程式

提供開發人員各種工具箱，以便他們將最新的鑑別方法整合至新的應用程式中。

啟用使用者生命週期管理

簡化內部部署和雲端應用程式的使用者上架、下架和自助式存取要求等原則。

讓經理通過委派而有能力控管存取權限

縮減 IT 時間與技能的相依關係。將應用程式所有權的責任委派給事業單位管理者，讓他們能夠提供員工更快速的應用程式存取。

充分利用您的內部部署 IAM 投資

整合常用的內部部署目錄，例如 AD/LDAP。

與 IBM Security Access Manager 無縫整合

單擊啟動讓 IBM SecurityAccess Manager(ISAM) 使用者可立即存取 IBM Cloud Identity。

IBM Cloud
Identity

精選案例

美國鐵路公司透過改善身份辨識管理進而保護企業營運

業務挑戰

美國鐵路公司透過將改進身份辨識管理來確保營運正常運作。因原身份辨識與控管舊版軟體已經到期，公司決定尋求替換解決方案。尋求新導入產品必須不影響任何的現行業務活動下進行更換及切換。

導入成果

減少 30% 時間成本 ► 時間與成本同時降低，並且不需要和舊有系統併行運作。

大幅提高安全性 ► 通過新系統功能提高安全性，能辨識並讓正確的使用者登入，也阻擋非授權的入侵。

提高管理靈活度 ► 能輕鬆容易地新增新用戶帳號，也能在員工離職後刪除該員工的特權帳號。

客戶推薦

IBM 的新身份辨識及管理解決方案幫助美國鐵路公司管理企業內部使用者權限，以保護其重要資產。新產品導入時，對公司營運影響不大，這對於任何 IT 項目而言都是件非常重要的標準。其將遷移時間和成本減少了 30%，並且無需同時維護兩個新舊系統，大大改善用戶體驗。


IBM Cloud
Identity

IBM Cloud Identity

立即免費試用

或撥打 0800-016-888 按 1
立即聯絡 IBM 業務代表提供進一步協助

Key Point **4**

IBM Security Guardium

為滿足企業資訊安全、合規、稽核等需求，IBM Guardium 在法規遵從、資料可用、資料保留、資料安全四個方面來進行資料保護給予專項治理和加強，並簡化安裝部署工作，滿足企業資料庫更完整的稽核監控與即時保護。

您是否面臨 ...

數百個資料庫都需要滿足監管和合規要求、需要提高大資料專案的資安性和合規性，如 Hadoop、NoSQL 等，對安全合規和資料隱私權原則的重視度增加、期望在資安和合規策略方面變得更為主動，而非被動應戰；希望提升安全解決方案的自動化水準、也需要推動合規性，確保實現真正的安全性。

高效識別安全合規性風險，有效降低風險提高安全品質

滿足安全和合規要求的流程效率提升了 20%

使企業組織提升了滿足安全和合規要求所需流程的效率。導入後，企業改善了資料庫安全、審計協定和報告功能，並實現了自動化，使員工可更高效地處理安全需求。

降低遭主管機關罰款的可能性

導入 Guardium，企業滿足了廣泛的合規與監管法規要求如：實施 GDPR，並為其提供了有關敏感性資料更深入的可視性。如此一來，企業將遭受主管機關罰款的可能性降低到 2% 。

每年在資料外洩復原方面節省了超過 97,900 美元的成本

有助於導入監控和審計、漏洞管理、資料轉換、即時安全性原則和智慧化報告，從而識別和防禦內外部威脅。投資 Guardium 後的第 3 年，企業發生資料外洩的可能性降低了 45%。

避免了開發和支援內部監控和審計功能所需的人工成本

投資後，企業組織就無需針對如何安全地記錄、儲存、分析和 報告資料庫審計存取資訊進行開發、測試和部署替代性內部解決方案，進而節省了 960 個工時的企業成本。此外，企業還可以存取由 Guardium 提供的更健全功能。該公司省下了支援內部解決方案所需的 6 個全職員工。

IBM Security Guardium 四大關鍵要素

滿足企業合規報告和審計需求

企業需滿足合規和監管方面的需求，包括：HIPA，PCI/DSS，以及歐盟法規 GDPR 等。此外，能夠監控受權用戶並阻止未經授權的存取。某家金融服務機構的網路安全管理副總裁介紹說「通過 IBM Guardium，我們能夠獲得比之前更多的資料洞察力，也能夠更深入地瞭解存取資料的人員行為。」

提高敏感性資料的可視性

提高了對於敏感性資料的可視性，發現、瞭解資料並進行分類。企業資料每年增長率高達 20%，更顯資料洞察力是確保資安的關鍵。敏感性資料難以洞察，而可幫助發現潛在的問題來源。隨著企業承擔更多的大資料專案，資安威脅倍增，此時更好地瞭解敏感性資料的所在位置愈發重要，能助其在企業資安方面做出比以往更明智、更好的決策。

完整保護整個企業環境內的敏感性資料

通過即時保護工具，可以降低員工從事非預期存取的風險，而通過原生的記錄功能，就可能會遺漏這些存取。也能夠持續監控整個企業環境內的存取，確保資料庫、資料倉儲、Hadoop、NoSQL 以及檔共用庫等各種資料儲存系統的安全。此外，它還有助於確保各類資料的安全，無論資料是儲存在內部或外部，或儲存在大資料環境、私有雲或混合雲環境中。通過部署集中式解決方案來監控各個平台，帶來巨大業務價值。

通過與該領域強大的合作夥伴開展合作，創建可靠環境

與市場領導者的合作提升可靠性，可擴展的解決方案意味著無需聘請額外人力，便可支援不同規模的環境；同時，由於其非侵入式的設計，不會對企業資料庫或資料倉儲的效能產生影響。使得無需聘請新的人員，同樣規模的原團隊也能完成原本的日常工作任務。這代表企業可簡化營運，同時提高企業資安性原則的品質。

IBM Security
Guardium

精選案例

幫助 Morneau Shepell 全球最大型的員工協助計畫保護公司敏感數據

無論您的問題屬於何種性質
Guardium 將能保護您所有在安全規範內的資料

業務挑戰

Morneau Shepell 全球最大型員工協助計畫，需要找到可信賴的資安解決方案，因其缺乏對於何種資料存在風險、哪些資料可能導致毀滅性安全威脅的可視性。因此，企業需要保護各種環境內的結構化資料和非結構化資料的安全並確保做到合規，包括內部環境、外部環境、私有雲環境、公有雲環境或混合雲環境、主機環境或者大資料環境等等。

導入成果

節省 20% 時間 ► 在應對安全和合規要求方面能節省 20% 的時間。

降低 45% 資料外洩風險 ► 資料外洩可能性降低到最低 45%。

節省 6 名員工人力成本 ► 可在未來避免雇用的員工數量減少到六個以下。

客戶推薦

企業組織發現，通過與該領域強大的合作夥伴開啟合作，能創建可靠的環境。IBM Guardium 是資安與合規性領域值得信賴的市場領導者，受訪企業組織表示，透過導入 Guardium 提升了可靠性，使得他們對資安充滿了信心。此外，可擴展解決方案意味著，無需聘請額外的人力，便可支援不同規模的環境；同時，由於其非侵入式的設計，它不會對企業組織資料庫或資料倉儲的效能產生影響。某家金融服務機構的網路安全管理副總裁也談到，「我們之前的解決方案不能很好地擴展。現在，透過 Guardium，即便我們新增了一些資料庫，但也無需聘請新的人員，原同樣規模的團隊也能完成他們的日常工作任務。」

IBM Security Guardium

加速實現端對端 提高資料防護能力

發現
橫跨複雜的資料環境，發現資料並予以分類。

監控
即時監控整個環境的資料存取情形。

管控
管控權限，防堵未經授權的存取。

鞏固
鞏固資料防護能力，為最敏感的資料設下存取限制。

防護
保護閒置與使用中的資料。

IBM Security Guardium

瞭解更多

或撥打 0800-016-888 按 1
立即聯絡 IBM 業務代表提供進一步協助

Key Point **5**

IBM Cloud Pak for Security

實現業界首次無需從原始資料來源移動資料而能連接任何友商安全工具、雲和本地部署系統，IBM Cloud Pak for Security 為 IBM 首創開源新技術的資安平台，能夠搜索並轉換來自各種來源的安全資料，彙集企業多雲 IT 環境中的關鍵安全洞察做整合，並在統一的介面下把安全工作流程與自動規程連接起來，讓安全部門能夠更快地對資安事件做出快速並自動化地回應。

快速回應跨雲網路威脅的開放平台

隨著越來越多業務運作移至雲端，安全資料往往分散在不同的工具、雲端及 IT 環境中。
需要團隊花更多時間整合工具與資訊，而且還需要維護這些整合，因此保護組織的時間反而變少。
IBM Cloud Pak for Security 協助團隊利用開放的安全平台來解決這些問題，串連所有片段的資安工具。

專為混合、多雲環境設計的安全

Cloud Pak for Security 支援跨任何雲或者本地環境，能輕鬆地實現「容器化」部署。隨著企業不斷增加新的雲部署和遷移，Cloud Pak for Security 可以輕鬆地適應這些新環境並支援不斷擴展 - 客戶甚至能夠將敏感和關鍵任務工作負載放到雲中，在中心安全平台上持續監視這些負載，並進行控制。

開放彈性的高效部署整合

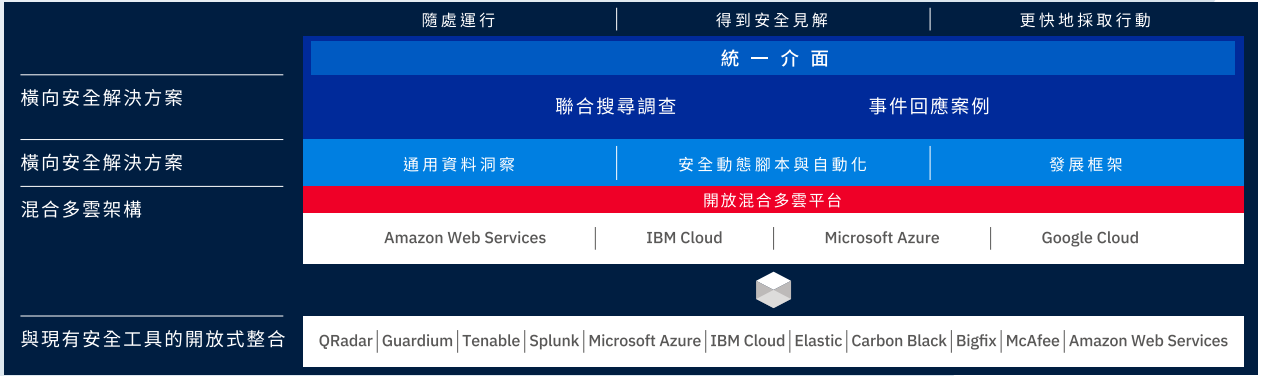
IBM Cloud Pak for Security 實現業界首次無需從原始資料來源移動資料而能連接任何友商安全工具、雲和本地部署系統。由預先與 Red Hat OpenShift 相整合的儲存容器化軟體所組成。

統一介面進行洞察威脅及 IOC

此平台透過使用開放式標準來連接您現有的安全工具，以便您搜尋混合式多雲端環境中的威脅指標。它還會使用統一介面來連接全公司的工作流程。

IBM Cloud Pak
for Security

IBM Cloud Pak for Security 跨雲整合 自動化回應



在不移動資料的情況下獲得安全洞察

為進行分析而傳輸資料會帶來額外的複雜性。IBM Cloud Pak for Security 能夠連接所有資料來源，以發現隱藏的威脅，進而做出更好的基於風險的決策，而無需移動資料。利用 Cloud Pak for Security 的 Data Explorer 應用，安全分析師能夠非常順利的跨任何安全工具或者跨雲來搜索威脅。如果沒有此功能，安全部門將不得不在每一個單獨的環境中手動搜索相同的威脅指標（例如惡意軟體簽名或者惡意 IP 位址）。Cloud Pak for Security 是業界第一款不需要將資料移轉至平台即可進行分析以支持此類搜索的工具。

自動的快速回應安全事件

IBM Cloud Pak for Security 在統一的介面下把安全工作流程與自動規程連接起來，如此安全部門能夠更快地對安全事件做出回應。該平台支援企業編排數百種常見安全場景的回應，指導用戶完成整個過程，用戶能夠迅速存取適用的安全資料，使用合適的工具。IBM 的安全編排 (Orchestration)、自動化 (Automation) 和回應 (Response) 功能與 Red Hat Ansible 整合，提供更多的自動化規程 (playbooks)。透過規範整個企業的安全流程和活動，企業能夠更快、更有效地做出回應，同時為自己提供加強監管審查所需的資訊。

可在任何地方運行，開放的安全連接

IBM Cloud Pak for Security 可以輕鬆地安裝在任何環境中，無論是本地、私有雲還是公有雲。它提供的統一介面簡化了操作，由預先整合 Red Hat OpenShift 的容器化軟體組成 - OpenShift 是行業最完整的企業級 Kubernetes 平台。

IBM Cloud Pak
for Security

IBM Cloud Pak for Security

立即諮詢

或撥打 0800-016-888 按 1
立即聯絡 IBM 業務代表提供進一步協助

IBM X-Force

Cyber Tactical Operations Center

行動式資安戰情中心 C-TOC

公司如何為資安危害做準備

IBM X-Force C-TOC 是一個可全面運作的行動式資安戰情中心，它仿照軍方使用的「戰術作業中心」，以及首批應變人員所使用的事件指揮站。這個設在牽引式聯結車內部的行動式設施提供由手勢控制的網路安全「觀察室」、資料中心與會議室，裡面可容納二十幾位作業人員、分析師與事件指揮中心人員。此設施可部署在各種不同環境中，擁有自給自足的電力、衛星及蜂巢式通訊，可提供無病毒並具復原力的網路，以供調查與回應之用，同時提供最現代的平台以利進行網路安全訓練。

為公司的最壞情況做好準備

來自 IBM X-Force Command 的資安專家團隊與專業駭客能幫助企業訓練各種組織的危機應變 - 包括執法部門、情報機構、許多全球各大銀行以及各大能源和技術公司。以逼真的沈浸式體驗，在模擬和遊戲化環境中提供重要的網路安全和領導技能，為組織的最壞情況做好準備。現在就來預約並親身體驗 IBM X-Force Command 的威力吧！


X-Force Command
Cyber Tactical Operations Center
IBM Security
IBM Security
X-Force Co

X-Force Command 專為您量身打造的獨特體驗

X-Force Command Cyber Range

全球唯一能容納所有事故現場指揮人員和融合團隊的全面實境網路靶場。體驗由精英訓練小組引導企業負責人員的身歷其境模擬。地點在美國麻州劍橋市。

行動式資安戰情中心

IBM X-Force Command 網路戰術行動中心 (C-TOC) 是一種獨一無二的行動式網路體驗，它可以配置為網路靶場、執行網路調查戰情室、或針對特殊安全事件的現場網路監視樓層。目前在歐洲巡迴中。

IBM 客戶體驗中心

與經驗老到的事故應變人員、滲透測試人員、設計思考專家和 IBM 高階主管會面，以建置及磨練您的網路安全與事故應變策略。

作戰從演練危機應變開始

立 即 瞭 解 更 多

進一步瞭解 IBM 解決方案
請致電 0800-016-888 轉 1
或立即聯繫貴公司專屬之 IBM 業務代表