POWER9™ 的層層安全把關作法

保護並優化 IT 基礎架構也能順暢無礙

業務代表為您服務：

+886 80 001 6888 按 1

註冊告訴我們您的需求：

https://ibm.biz/BdqM7X

敬請訪問網站：

https://ibm.biz/BdqM7H

IBM **Power Systems**

IBM

在網路攻擊猖狂的時代，企業 IT 該如何自處

狂妄放肆的資料外洩事件深具毀滅性，安全性已成為許多高階主管現今最該謹慎對待的要務，因此不少組織的安全預算不斷往上墊高。可是增加的支出和技術改革至少有部分帶來了新的複雜性與風險，反而對 IT 安全性造成威脅。根據 2019 年 Forrester 對於安全專家的問卷調查發現，「低於四分之一」的預算就能讓他們「完全滿意自己的安全產品組合，以便支援他們開發進階威脅情報功能、提高安全人員的生產力、擷取資料中的洞察見解並提升效率。」[1]

安全專家主要關心的問題是，不斷攀升的攻擊次數和狡猾手法，讓現今企業曝露的層面比以往多出更多。才在不久以前，硬體與韌體層級內的漏洞並不是什麼需要大量關注的問題，可是如今卻發現這可是主要的攻擊目標。

同時，隨著 IT 架構持續進步，威脅將層出不窮的發生。在許多方面來說，企業必須克服的網路安全挑戰可以歸結為兩個實證真相：IT 堆疊擴展（這是直接結果）和駭客越變越高明。

目前威脅趨勢的最新真相

現今組織仰賴安全系統來保護智慧財產、機密企業資訊、機密個人資訊及隱私權，防止遭到威脅攻擊。所以如何機智地採取 IT 安全作法是刻不容緩的一件事。

通常可以藉由採用商業、規範或財務導向的作法來達到安全性。雖然這種作法有其價值，可是卻無法提供充足的保護效力。讓商業程序能對抗層出不窮的 IT 系統風險。而且也可能會忽略關鍵跨領域層面。

理想的作法需要規劃和評估，才能找出各個關鍵領域的相關安全性風險。IBM Power Systems™ 和 POWER9 處理器提供全面性的層層安全策略作法，確保組織能安全無虞並遵守規範。這種層層安全作法包括以下項目

- 硬體
- 韌體
- Hypervisor
- 作業系統
- PowerSC

採用全面性安全作法可讓組織滿足目前影響安全趨勢的四個現實需求。

駭客變得越來越狡猾高竿。組織越是突破傳統內部部署資料中心的限制，空間網路攻擊者越會絞盡腦汁地奇招盡出。他們的攻擊手法不再侷限於網路層級，因此變得越來越高明、更高竿。

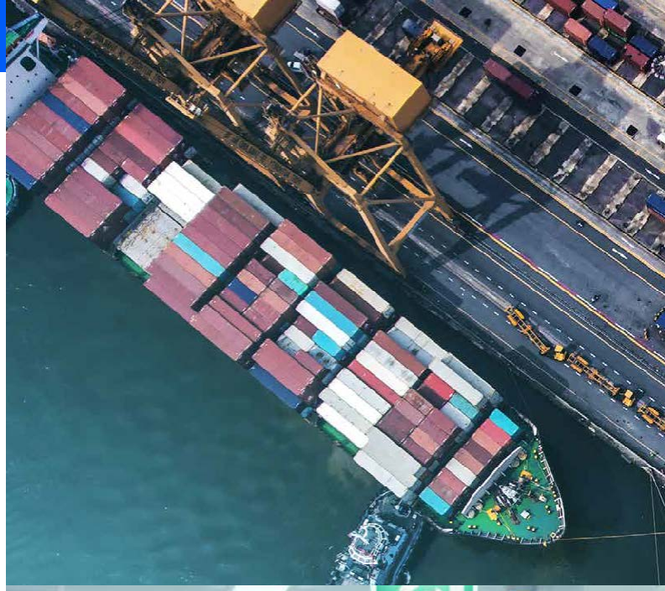
越來越多業務是在行動和邊緣裝置上進行。現在員工幾乎隨處都能儲存並存取組織內的資料，例如透過伺服器、混合雲環境及無數個行動與邊緣裝置。於是伺服器與裝置之間免不了來回貫穿交錯，是現在數位轉型造成的副作用，也產生了全新的攻擊向量，隨時都能遭到入侵。

規範日益嚴苛，風險設定檔也受到影響。用來確保符合規範的安全程序也會無意間造成風險曝露的問題。

這種增長趨勢讓歐盟的 GDPR 有了最新的發展結果：受到控管的實體要更密切留意組織使用資料的方式。可是這也讓平常的業務運作變得更複雜。

員工就是隨時會發生的漏洞。不論您實施了什麼安全控管作法，或漏洞管理有多滴水不漏，員工隨時都有造成一定風險的可能。就算您很努力地保護端點安全，乖乖遵守規範，還是可能因為某個無心之過或高明的惡意攻擊而飽受爭議。同時，不少組織都在尋尋覓覓、努力留住厲害的安全人員，可是卻發現自己永遠缺乏安全技能。

隨著 IT 架構持續進展並順應不斷變化的技術潮流、工作文化和規範，現今的網路威脅只會層出不窮、變本加厲，而且肆虐速度更快。這代表您的安全策略也必須加碼改進，才能超越網路層級。



全面性的層層安全作法是必要的

透過實作各種第三方廠商的安全解決方案，就可以把安全性內建於每一層堆疊中。不過這種作法卻會加重既有的複雜性，在網路中引來更多漏洞和曝露點。所以最好的辦法就是採取全面性層層作法，一個能保護所有組織資料與系統，同時徹底降低複雜度的作法。

考慮到這一點，因此 IBM 打造了 IBM Security Framework，在使用全面性業務導向的安全作法時，能協助確保 IT 每一安全層面都能受到妥善因應。

IBM Security Framework 擅長保護以下項目：

1. **基礎架構**—以使用者、內容及應用程式的洞察見解，防範狡猾的攻擊。
2. **進階安全與威脅研究**—透過保護技術，洞悉漏洞狀況與攻擊方法並加以應用這個洞察見解。
3. **人員**—運用綜合性的身分情報在安全網域之間管理並延伸企業身分驗證。
4. **資料**—保護組織最授信資產的隱私和完整性。
5. **應用程式**—降低開發更多安全應用程式的成本。
6. **安全情報與分析**—以額外的環境定義、自動化及整合方法，優化安全功能。

進一步瞭解 IBM Security Framework 並閱讀 IBM Security Blueprint 瞭解深入知識。

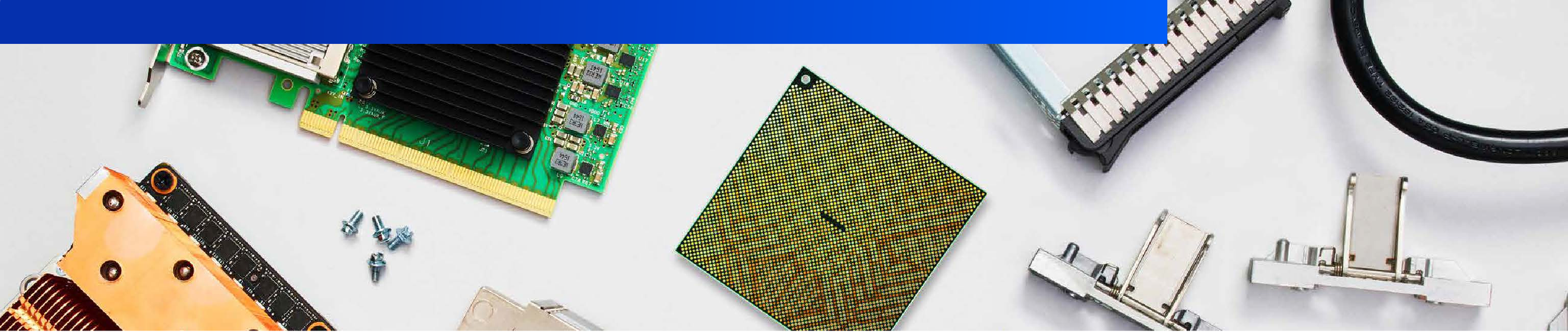
IBM Power Systems 與 POWER9 如何保護堆疊

有了 IBM Power Systems，您就能獲得緊密整合完整堆疊的綜全性端對端安全功能，舉凡處理器、韌體、作業系統、Hypervisor、應用程式、網路資源，一直到安全系統管理等等全都在保護範圍內。

硬體、韌體、Hypervisor

24 個加密引擎

POWER9 處理器的加密引擎比 POWER8® 前版處理器多出一倍。您可以在層層堆疊之間用雙倍的速度或更快加密靜態或動態的資料。



晶片加速器

POWER9 標榜擁有晶片加速器，能比軟體更快壓縮和解壓縮 GZIP 檔案。您可以快速壓縮和加密整個虛擬機器，並在網路之間安全地移動。

POWER9 安全開機

安全開機功能會透過數位簡章來確認和驗證所有韌體元件，以便保護系統完整性。IBM 發行的所有韌體都經過數位簽章和驗證。您也可以安裝自己的韌體並取代驗證所需的公開金鑰階層。

信任開機與信任平台模組 (TPM)

POWER9 中的信任開機功能可以對伺服器上的所有韌體元件進行檢驗和遠端驗證（證實）。信任開機功能會使用 TPM 這個擁有「信任根源」(Root of Trust, RoT) 的作用來衡量軟體堆疊。TPM 本身就會簽署驗證，讓您知道韌體並未遭到任何方式的竄改。

IBM PowerVM® 企業 Hypervisor

IBM PowerVM 的安全追蹤記錄比主要競爭對手都要更卓越，因此您可以放心保護虛擬機器 (VM) 與雲端環境。

作業系統

IBM Power Systems 為各式各樣的作業系統，例如 IBM AIX®、IBM i、Linux® 提供領先的安全功能。視作業系統而定，功能也不盡相同，例如以下範例：

- 指派通常保留給 root 使用者的管理功能，而不犧牲安全性
- 透過個人金鑰儲存庫加密檔案層級的資料
- 更能掌控使用者可用的指令與功能，同時掌控使用者能存取的物件
- 運用使用者與物件的系統值和物件審核值，在安全審核日誌中記錄物件的存取狀況
- 將整個磁碟機完全加密，首先會加密物件，然後以加密形式編寫出來
- 每個檔案要先經過衡量和驗證之後，才能執行或開啟供發出要求的使用者使用。

工作量、虛擬機器及容器

工作量不再受限於內部部署資料中心，而是持續移動至虛擬化及雲端環境中。這代表許多組織都紛紛採用容器在混合式基礎架構之間部署全新和現有的應用程式。這些日益動態的環境和工作量需要同樣多用途的安全功能。

即時分割區行動性 (LPM)

IBM Power Systems 能保護動態中的資料。當您需要在系統間移轉時，LPM 會透過加密功能來保護虛擬機器。如果您已虛擬化內部部署資料中心和/或混合雲環境，那麼這個功能就相當重要。

受保護的執行設備

受保護的執行設備就是 IBM Power Systems 保護這個堆疊層級的一個例子。它是由 POWER9 功能在安全的記憶體中加密並執行虛擬機器，意思是說已受損的 Hypervisor 將不會有存取權限。此外，在雲端環境中，擁有虛擬機器存取權限的惡意內鬼或管理者將不能存取在安全記憶體中執行的工作量。解密程序只會在經過驗證的系統中執行。

IBM Power Systems 上的整合式安全產品

IBM PowerSC™ 是針對雲端和虛擬環境中企業安全和規範的整合式產品組合供應項目。它位於堆疊之上，同時提供網路型的使用者介面，管理位在最底層開始的 IBM Power Systems 安全功能。

IBM PowerSC 能縮短時間、成本及風險

有了簡化和自動化的功能，IBM PowerSC 就能協助簡化規範與審核處理程序，進而節省時間並削減成本。還能促進堆疊之間的監控能力，藉此降低安全風險。

IBM PowerSC Standard Edition 功能

規範自動化

IBM PowerSC 隨附預先建置的設定檔，能支援一系列的產業標準。您可以自訂這些設定檔，並將其與企業規則合併，不必使用到 XML。

即時遵守規範

當有人開啟安全關鍵的檔案或與之互動時，就能偵測得到並發出警示。

信任網路連線 (TNC)

當虛擬機器不在預先指定的修補程式層級時就會發出警示。而且當修正程式變成可用時，還會再通知您。

信任開機

可以檢驗和遠端驗證在伺服器上執行的所有韌體元件。

信任防火牆

保護和路由 AIX、IBM i 及 Linux 作業系統之間的內部網路流量。

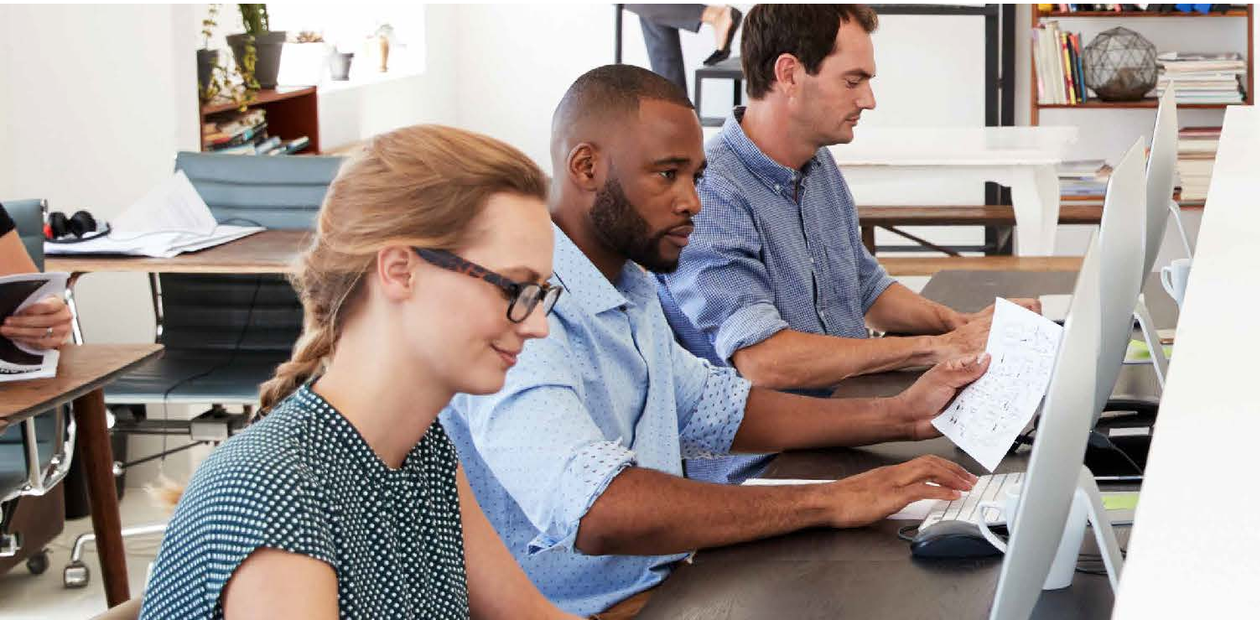
信任記載

建立集中式審核日誌，可以輕鬆備份、保存及管理。

預先配置的報告與互動式時間表

IBM PowerSC Standard Edition 支援審核五個預先配置的報告。您也會擁有互動式時間表可查看虛擬機器的情況和事件。

如需進一步瞭解 IBM PowerSC 的許多功能，請參閱下列 IBM 紅皮書「透過雲端與虛擬環境中的 IBM PowerSC 來簡化安全與規範的管理作業」。



最強大的安全作法就是簡單流暢

隨著駭客能力越來越狡猾高竿，而且技術發展也為現今企業招致新的漏洞，因此整合全面性的層層安全解決方案，又不增加組織複雜性，就變成了關鍵。IBM Power Systems 會透過同一家廠商緊密整合的深度解決方案，來保護每一層的堆疊。一個安全策略若仰賴多家廠商的多種組件，就會帶來複雜性，最終證實在更多方面代價更高昂。

只採用一家廠商的安全功能，可以簡化並加強安全策略，自然有其優勢。IBM Power Systems 建基於 30 年的安全領導地位，能引進與其他 IBM 內外組織深厚的合作夥伴關係，進一步厚實了其安全專業知識。這樣深厚的合作關係能讓 IBM Power Systems 融入更廣大的安全專家社群，確保能快速察覺問題並且有把握地加以解決。有了 IBM Security 與 IBM Research 事業單位作為後盾，加上 PowerSC 產品組合，POWER9 伺服器就能從頭到尾徹底對抗多種威脅，包括內鬼攻擊。

運用全面性層層作法簡化整個堆疊之間的安全性，保護企業安全無虞。

若要進一步瞭解 POWER9 伺服器如何協助保護基礎架構，請立即預約諮詢。

業務代表為您服務：

+886 80 001 6888 按 1

註冊告訴我們您的需求：

https://ibm.biz/BdqM7X

敬請訪問網站：

https://ibm.biz/BdqM7H

1. 2019 年 5 月 Forrester Research, Inc「2019 年網路安全報告的複雜性：降低複雜性如何帶來更好的安全成果」。

IBM Systems, 11501 Burnet Road, Austin, Texas 78758

85028385USEN-00