

**BlackBerry** Intelligent Security. Everywhere.

# BlackBerry UEM Suite

適用於數位工作場所的零信任安全解決方案

解決方案簡介



「BLACKBERRY UEM 在 GARTNER® PEER INSIGHTS™ 的統一終端管理工具類別中，獲得 2023 年客戶首選供應商的表彰。」

## 網路防禦前線的零信任行動優先安全解決方案

對組織及其員工而言，要迎向終端管理和安全性的挑戰，需要的是複雜縝密、經過證實的安全性優先作法。

# 101%

增幅：與四大用戶端 OS 有關的提報漏洞數<sup>1</sup>

# 48%

的知識型工作者將在 2023 年底前全面採用混合式工作方式<sup>2</sup>

# 67%

的受訪組織受到內部威脅的影響<sup>3</sup>

## 告別附加式安全解決方案

BlackBerry UEM 自建構之初就十分注重安全性。

## 擁抱聚合型安全性框架

為網路防禦前線提供有效的零信任安全性。

## 隨著工作場所需求的動態變化一起演進

確保 BYOD 的功能和相容性皆正常運作，並適用於最廣泛的安全應用程式。

## 確保合規性

具備領先業界的認證及鑑定。

## BLACKBERRY UEM SUITE 提供了安全性和彈性

針對組織多元且不斷變化的裝置群 (其可能選用最廣泛、企業隨即可用的應用程式和重要應用程式)，BlackBerry® Unified Endpoint Management (UEM) 透過完整的終端管理和政策控制來實現安全生產力。透過單一管理主控台，生產力應用程式套件和可靠的端對端安全模式，BlackBerry UEM 提供的彈性和安全性可確保員工安全連線並維持生產力，如此一來，他們幾乎就能使用任何裝置，在任何地方辦公了。

## 終端管理的現代作法

BlackBerry UEM Suite 提供了安全性和生產力的完美平衡，同時也實現了零信任安全性和防護。

終端	擁有權模式	作業系統	安全和管理選項	應用程式和平台	內容儲存庫
	BOVD (自攜裝置)	iOS	BlackBerry Dynamics	BlackBerry Work	BlackBerry Workspaces
	BOYL (自攜筆記型電腦)	Android	CylanceENDPOINT	Office 365	OneDrive for Business
	COPE (企業擁有、個人使用)	Windows	CylanceEDGE	App Store Google Play Store	Box
	COBO (企業擁有、僅限業務使用)	macOS	Microsoft Intune	iOS Managed Apps	Microsoft SharePoint
			Samsung Knox	Windows Store for Business	
			Android Enterprise	AppConfig Community	ECM Repositories

## 行動裝置管理

重要平台和裝置擁有權模式的政策和控制項皆保持一致。

## 行動應用程式管理

在安全容器內將重要工作流程、業務流程和最廣泛的企業應用程式行動化。

## 為何要選擇 BLACKBERRY?

### 傳輸中數據的安全性

具備領先業界的連出即啟動單一連接埠連線能力，無需加裝額外元件。

### 靜止數據的安全性

透過公私加密分離技術來消除對主機 OS 的依賴，同時兼顧了使用者的隱私權和合規性需求。

### 升級使用體驗

確保 BYOD 的功能和相容性皆正常運作，並適用於最廣泛的安全應用程式。

### 滿足監管需求

為數最多的安全性認證及鑑定務，有助於您符合任何監管機構的規定。

### 管理和保護您的攻擊面

啟用和部署終端安全解決方案，發揮除終端管理之外的其他潛力。

## 行動內容管理

使用原生文件編輯，從內容儲存庫存取您的業務檔案。BlackBerry® Workspaces 能保衛防火牆外的檔案，它具有內建數位版權管理 (DRM)，是一款安全的企業檔案同步和共享 (EFSS) 解決方案。

## 身分與存取管理

BlackBerry UEM Suite 透過 Microsoft® Active Directory® 整合、Kerberos、OIDC、SAML 瀏覽器存取權支援和適用於安全應用程式的雙重驗證選項，藉此納入身分與存取管理 (IAM)。

## 部署彈性

適用於 BYOD 和企業自有裝置的內部和雲端部署，隨時隨地支援任何裝置上所有可能的部署用例。

## 零信任網路存取

實施最低權限的動態網路存取模式和基於身分的自適應控管措施 (零信任架構的重要元件)，藉此改善整體風險態勢。

<sup>1</sup> IDC - IDC 對 CVEdetails.com 提報的 2011-20 年 Windows、macOS、iOS 和 Android 漏洞之分析

<sup>2</sup> Gartner - 預測分析：全球知識型員工的混合式、完全遠端和現場工作方式 (2023 年 1 月)

<sup>3</sup> Ponemon 研究機構 - Ponemon 2022 年內部威脅報告 (2022 年)

© 2023 Gartner, Inc. Gartner® 和 Peer Insights™ 皆為 Gartner, Inc. 及/或其分支機構的商標。版權所有。Gartner Peer Insights 內容包含了個別終端使用者基於其自身經驗的意見，不應解讀為事實陳述，這些意見也不代表 Gartner 或其分支機構的看法。Gartner 不對本內容所述的任何供應商、產品或服務背書，也不對本內容的準確或完整性做出任何明示或暗示保證，包括適銷性或特定目的適用性的任何保證。

 **BlackBerry**® Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) 為世界各地的企業和政府提供智慧安全軟體與服務。本公司保護超過 5 億個終端，包括 2 億 1 千 5 百萬輛以上的汽車。本公司總部設於加拿大安大略省滑鐵盧區，在網路安全性、安全和資料隱私權解決方案領域中，利用人工智慧和機器學習提供創新的解決方案，同時是終端安全、終端管理、加密和內嵌系統等領域的領導企業。BlackBerry 的願景十分明確，那就是開創您能信任的互連未來。

© 2023 BlackBerry Limited. 商標，包括但不限於 BLACKBERRY、EMBLEM Design 和 CYLANCE，為 BlackBerry Limited、其子公司和/或分支機構之商標或註冊商標，依據授權使用，且明確保有該商標的專屬權。所有其他標誌皆為個別擁有者的資產。

如需更多資訊，請瀏覽 [BlackBerry.com](https://www.blackberry.com) 並且關注 [@BlackBerry](https://twitter.com/BlackBerry)。

