**電子書**

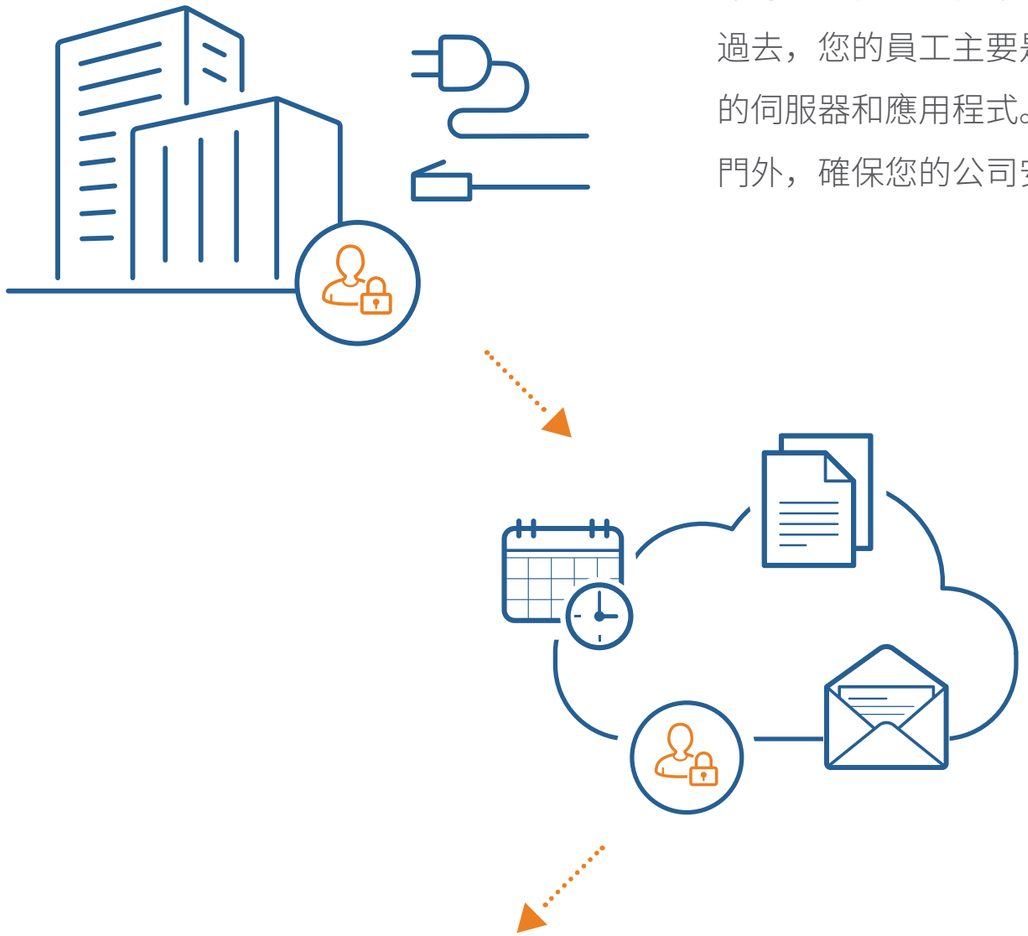
# 身份安全：不容忽視更是當務之急

*勇往直前**而無後顧之憂。***

CYBERARK®

# 內容目錄

# 1 我們如何演變至此

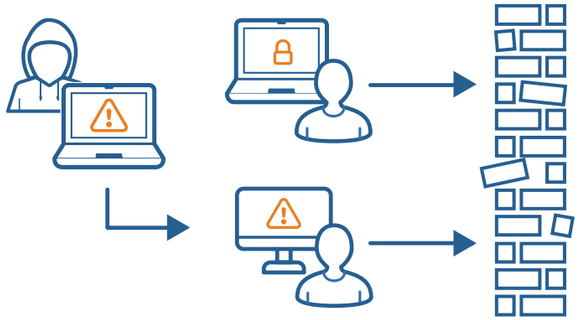


## 以往的安全系統沒那麼複雜

過去，您的員工主要是到經營場地上班或透過 VPN 連線。他們從公司自有個人電腦存取同樣也在現場的伺服器和應用程式。需要存取關鍵業務資源的人員較少，只要建立強大的安全邊界便能將惡人拒之門外，確保您的公司安全無虞。

## 數位轉型成為大勢

為了提高競爭優勢，公司開始迅速採用以雲端為架構的技術及服務，為客戶提供吸引力十足的數位體驗。我們也見證到，分散式工作團隊獲得越來越有力的支援。這些趨勢都在 2020 年爆發性成長，只有數位業務強大的企業組織能夠蓬勃發展。



## 原有的邊界已式微

隨著數位創新崛起的新技術及其用戶，使得以邊界為基礎的安全做法逐漸捉襟見肘。現在每一個客戶、遠距員工、裝置及應用程式都可能需要一個進入您最敏感系統的入口點。不僅如此，我們正身陷全球疫情，所有人都逼得倉皇加快步伐，忙於連接住家辦公室的網路、支援新裝置及確保新的協作工具儘快上線。數千個入口點使您的網路邊界更加脆弱，網路攻擊者也很清楚這一點。

## 攻擊次數暴增

**400%**

網路攻擊通報數量的增長率

*FBI，2020 年 4 月*

**667%**

魚叉式網釣攻擊的增長率

*Barracuda，2020 年 3 月*

**800%**

勒索軟體攻擊的增長率

*MonsterCloud，2020 年 8 月*

## 新篇章的開啟

數位轉型為企業開創許多新機，但也為攻擊者敞開了大門。網路攻擊或許無可避免，但我們能避免攻擊損害業務。本電子書接著將概要介紹如何借助以身份為核心的安全模型，在當下的新威脅情勢下提高您的靈活應變能力。

# 2 條條路徑通向身份

在現今的混合雲及多雲世界裡，身份是新的安全邊界。
傳統的網路安全屏障已不足矣，所有身份都可能成為攻擊組織最寶貴資產所使用的途徑。

## 任何身份

- ✓ IT 管理者
- ✓ 供應商
- ✓ 機器身份
- ✓ 員工
- ✓ 客戶

從混合雲至多雲端工作負載的業務應用程式，以至於整個開發維運流程，其中的身份不論數量還是種類都日益增多，您需要採取以特權存取為基礎的新做法來保護上述身份的安全。

**79%**

**的企業過去兩年內曾發生與身份有關的資料外洩事件**

*2019 年 12 月。身份狀態：安全團隊如何應對風險*

# 身份攻擊手法解析

## 第 1 步：取得一個身份（任何身份）的有效憑證組合。

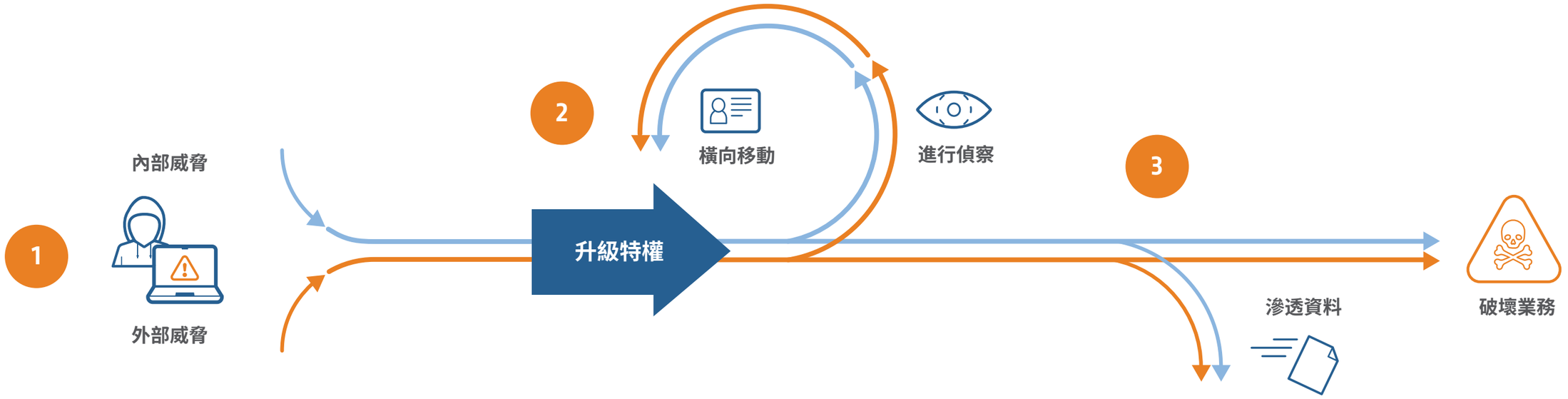
攻擊者可使用多種方法建立初始入口點，而侵佔身份就特別有效。最有效的技巧之一便是網路釣魚或社交工程陷阱，誘導員工洩漏其用戶名稱及密碼。最常見的漏洞還包括：內部威脅及不安全的應用程式碼，憑證被寫死且無意中暴露給攻擊者。

## 第 2 步：橫向及縱向移動以升級特權。

取得新的入侵管道之後，攻擊者便會進一步散播蠕蟲，在身份、應用程式與系統之間移動，尋找更高的存取權限。特權不斷升級，直到攻擊者到達其最終目標：內含關鍵業務資產（例如客戶資料和機密智慧財產）的系統、應用程式及資料庫。

## 第 3 步：攻擊。

高級別的特權存取權到手之後，攻擊者便會開始滲透您的關鍵客戶、財務數據或智慧財產。不然，攻擊者就會恫言關閉系統或洩漏敏感資料以換取贖金，就如最近新聞頭條頻頻報導。無論何種方式，結果都一樣：本已忙得不可開交的安全團隊，還要為昂貴且艱辛的補救措施耗費大量心力。



## 抱持「假定入侵」的心態

隨著傳統網路安全壁壘逐漸瓦解，您的業務很可能早已被侵入。現在該知道的是，情況已經如此，但您是否仍受到保護？這便是零信任做法的前提，我們將在第 4 章進一步討論。以您網路內的任何身份（人類或機器身份）可能都已被侵佔為前提，接著就可將注意力投向辨識、隔離並遏阻威脅者侵佔身份及取得特權，免其為非作歹。

# 3 身份兩大因素並重：速度 VS 安全性

隨著數位化步伐持續加快，有效的安全策略必須能與企業快速發展及流暢運作的業務需求相輔相成。

要求用戶重複對系統及應用程式進行身份驗證及保管多個複雜密碼不僅麻煩，而且費時。IT 團隊起碼得耗費大量時間處理密碼重設、帳號解鎖以及為用戶提供新的軟體和工具。最糟的情況是，員工會想盡辦法取巧繞過您辛苦設置的控制程序，或避免完全使用公司許可的系統及應用程式。

簡言之，企業發現自己在兼顧所有系統及資料安全與保持團隊高效工作之間進退兩難。他們亟需一個兩全的解決方案。這樣的解決方案，既要能給予用戶以快速、高回應效率及輕鬆的方式存取所需一切的權限，同時還能持續確保安全及遏制攻擊者。

「速度是企業的新貨幣。」

*Marc R. Benioff，*
*Salesforce 董事長兼執行長*

## 兼顧開發維運流程的各項要求

接納數位創新也意味著接納開發維運，開發人員及 IT 團隊須高度依賴自動化及雲端服務來加速創新及軟體發佈。但這個流程的安全防護往往無法面面俱到。通常，團隊會將特權憑證直接寫死至程式碼內並依賴工具的原生安全組件保護安全，甚至未將安全列為優先目標。他們或許也想到注重安全，只是苦於不了解特定的安全需求。

於是，應用程式及機器身份使用的憑證及金鑰便成了攻擊者唾手可得的目標。而且，由於安全問題通常留到流程結束後處理，開發人員對於臨時修改程式碼及延遲發佈備感壓力。

「應該思考：如何讓我的開發人員能不扼殺靈活度而把事情做好做對？」

*Fred Gibbins，美國運通公司資深副總裁兼資安長*

# 4 透過身份安全實現零信任

傳統的邊界式安全講求分辨善惡，並假定資料中心內的系統及流量可信任；而零信任假定惡意者已在您的網路內，並可存取您的應用程式和系統。

**在零信任模型下，授予存取權之前會驗證每個身份並授權。**

**驗證每個用戶**

**驗證每個裝置**

**智慧化限制特權存取**

零信任並非單一的技術，而是一種手法。其確保確認每個用戶的身份並驗證其裝置，且其存取權已經智慧化處理，僅給予所需權限，不再需要時權限便會取消。

身份安全提供一系列技術作為零信任做法的基礎。Identity Defined Security Alliance（身份定義安全聯盟）備有**實用的框架**，幫助我們了解需要身份級別保護的技術組件 – 從裝置到網路、應用程式及儲存空間。

**如能將身份安全結合人員及流程的適當調整，企業最後就不再需要在安全性與業務靈活性之間二選一。**

**71%** 已對身份所有權管理進行組織變革

*2019 年 12 月。身份狀態：安全團隊如何應對風險*

# 定義明確的身份安全

身份安全的重心在於保護整個存取關鍵資產週期中的個人身份。這意味著準確**驗證**該身份、身份只獲得適當的**授權**，並以有條理和系統的做法提供該身份存取特權資產的權限，以可**稽核**或歸責的方式確保整個流程周全得當。

## 嚴格驗證

- 情境式、依據風險且自適應的存取管理（SSO、MFA、LCM）
- 強大的無密碼驗證要素，包括生物辨識、行動推送及 USB 令牌

## 情境式授權

- 保護人類用戶、應用程式及其他非人類身份的特權存取
- 在所有平台、終端及應用程式上實施最小特權及即時存取原則

## 無摩擦存取

- 管理、配置、啟用存取及保護所有身份與資源類型的單一虛擬控制介面
- 自動化工作流程及自助服務（例如應用程式存取、用戶配置、帳號及密碼重設）

## 稽核與可歸責性

- 保護中介式連線以確保可歸責、監控/識別風險及產生防篡改稽核軌跡
- 風險分析可即時監控存取活動並針對可疑行為採取行動

## 無縫整合

- 與您現有的技術推疊（包括第三方威脅情報及開發維運工具）無縫整合
- 透過 API、SDK 及教程提供強大的開發人員支援

# 5 實現成功的路線圖

身份安全讓組織對自己最重要資產的安全感到安心，並可提高業務靈活性。不過，如何開始往往最令人頭疼。

CyberArk 藍圖是實現成功的身份安全之最佳實作框架。它為使用傳統地端基礎設施及軟體開發方法的組織及展開數位轉型計劃的組織制訂身份安全控制及最佳做法。組織使用藍圖儘快識別及解決其最大的身份安全風險，同時建立一個符合未來需求的身份安全計劃。

藍圖以事件回應的經驗心得及 CyberArk 實驗室團隊的尖端研究成果為基礎，提供廠商中立、可衡量、依風險調整的身份攻擊防禦建議。

## 規劃您的 CyberArk 藍圖課程

*請求免費評估*

Cyberark.com/blueprint

CYBERARK 是特權存取管理業界的全球領導者，提供最完善、靈活的身份安全功能。CYBERARK 保護任何身份（人類或機器身份）的存取安全，協助組織確保業務資產安全、保護其分散式員工團隊和客戶，以及加快雲端業務。

U.S., 02.21

CYBERARK®