citrix

Case Study

化轉機為典範

第一銀行結合 Citrix 領先金融業實現虛擬隔離上網

導入 Citrix Virtual Apps and Desktops 所獲得的最主要成效，第一個就是員工有了一個安全的上網環境，第二個則是員工作業電腦直接對外的連網途徑被阻絕，讓駭客無法遙控，從資安的角度，這是非常重大的成效。

— 第一銀行數位安全處處長 張晉榮

行業：金融產業

企業介紹

創立於1899年，目前隸屬於第一金控集團下的第一銀行，經營迄今已逾百年，總資產及第一類資本排名世界前三百大。目前在世界各大城市與金融商業中心均設有服務據點，可配合客戶經營需求，提供全方位金融服務。該公司秉持「顧客至上、服務第一」的經營理念，爲客戶的財富與託付創造更多的價值，期許能成為活躍亞洲的區域型銀行，給予客戶最滿意之金融服務、股東最豐碩且穩健之獲利、員工最佳的生涯發展空間。

挑戰

自從2016年爆發ATM遭到駭客入侵之後，第一銀行開始著手規劃強化整體資安防護能力的策略，而實體網路隔離則是最有效的方法之一。由於海外分行業務較單純，且核心銀行系統是放在第一銀行台灣總部，所以在第一時間便能啟用實體網路隔絕策略，並設立公共上網區解決需要存取網路資源的工作需求。相較之下，台灣各分行均設有核心業務系統，各分行、總行之間的資料交換頻繁，加上員工必須使用工作電腦上網查詢各項資料，因此無法採用實體網路隔離的策略。在此狀況之下，引進虛擬隔離上網解決方案，杜絕駭客入侵實體電腦的可能性，變成為第一銀行強化資安防護的最佳解決方案。

解決方案

為徹底解決資安問題，第一銀行透過詳細POC流程進行測試，最終引進 Citrix Virtual Apps and Desktops 解決方案，並將7,000位員工的傳統上網方式從個人電腦的瀏覽器改為透過 Citrix 虛擬上網瀏覽器，實踐虛擬隔離上網機制策略。

危機就是轉機，而能記取經驗並即時應對者，更能成為業界的典範 ---- 這正是第一銀行領先國內金融業界，率先導入 Citrix 虛擬隔離上網技術的最佳寫照。

當 2016 年 7 月第一銀行發生大規模 ATM 盜領案件，並經警察單位及調查局協助快速破案後，由於確定駭客入侵的端點之一來自第一銀行倫敦分行，「我們在當年就迅速設立數位安全處，以進一步加強辦公室環境的資訊安全。」第一銀行數位安全處處長張晉榮表示，「那時候我們的想法之一，是希望將員工的電腦與外界直接隔離，讓任何駭客無法入侵到內部員工的實體機器」。

第一銀行海外分行員工的辦公電腦是不能上網，而是採用實體隔離方式，在分行辦公室裡規劃一個特別的上網區域執行相關的銀行服務業務。但國內有 188家分行、7,000 多位員工，需透過上網執行業務服務與作業項目眾多，資料下傳頻繁，在國內實施實體隔離政策比較不易。

但在日常工作中，由於台灣的員工都是用自己的作業電腦連結網路，總是會逛到一些惡意的網站，一方面員工並非專家，另一方面有些網站實在是假冒的很詳細，要分辨是否為惡意網站有其困難，點連一些圖片就可能將惡意程式帶進來，讓駭客藉此來入侵員工的電腦。

因此第一銀行數位安全處強化辦公室資安所設定的主要目標，就是找到一個可以讓同仁安全、平穩地上網，又達到不會阻撓業務、讓同仁作業非常方便的方法。 2017 年初，幾經評估，數位安全處決定在公司內部打造虛擬化環境，讓同仁透過虛擬瀏覽器應用程式存取外部網路資源，避免員工的用戶端電腦遭到病毒或勒索軟體的入侵。

勇於任事，領先挑戰虛擬上網的建置

虛擬的觀念，已應用在非常多的地方，虛擬上網在國外也有人使用，尤其是新加坡和日本的金融業對這方面其實頗有經驗，但台灣金融業之所以尚未引進，是因為要導入這種技術，概念上並不困難，但實作上有挑戰性。

其中的挑戰在於員工的作業電腦不會只有純粹上網這件事，還需連接印表機，讀取各種卡 (如晶片金融卡、健保卡) 的資料，上網的資料要能列印出來；建立虛擬環境之後，這些週邊設備都必須串接起來並確保其能互相溝通。此外，員工的作業方式、上網習慣都要稍微調整，也增加了推行的複雜度。

基於慎重原則，第一銀行組成此一專案的評估委員會，尋找 Gartner Magic Quadrant (魔力象限) 中相關領導者解決方案以及國內有經驗的合作廠商。產品評比的主要條件包括：

效益

・只需使用四台伺服器，就可以滿足7,000名員工的日常上網工作需求，大幅降低設備維護成本。

・Citrix虛擬上網主機本身並沒有硬碟，且各項資料均放在內網後台主機上，所以當員工從內部連到外部虛擬上網處理公務時，因為無法直接取得內部機敏資料，因此無須擔心會發生資料外洩事件。

・當員工需要從公司內部存取外部資源時，即便虛擬瀏覽器環境遭到惡意程式或勒索軟體感染，也不會感染其他內部電腦，且當虛擬瀏覽器環境關閉之後，惡意程式等也會一起消失。

・導入Citrix Virtual Apps and Desktops虛擬上網解決方案，不只有達到虛擬上網的目的，同時可以將TCO效益最大化，透過Citrix ADC內建的雙因子驗證，以及充足的授權，亦可以提供防疫居家/行動辦公同仁安全的虛擬辦公環境。

・操作方式簡單，大部分員工並非資訊專家，所以操作方式必須簡化，與員工原來的工作方式不能差異太多。

・滿足客製化的需求，並在使用既有設備和應用程式下提供高速效能，不能因為透過虛擬平台上網而拖慢上網速度。由於員工人數眾多，如需更換所有員工的作業電腦和應用程式，成本太高，所以必須在原有設備上讓員工能夠直接使用，使整個作業轉換流程平穩、透明，員工感覺不出任何變動。

・很重要的是，必須整合新增的資料清洗機制。由於大部分員工上網都有可能下載資料，而下載的資料中，包括Microsoft Office、PDF 或 Flash 等檔案，就可能把惡意程式帶進來，因此導入的虛擬上網解決方案必須能夠整合第三方廠商簡稱資料清洗的 CDR (Content Disarm and Reconstruction，內容威脅解除與重組) 技術。

產品評選過程還包括概念驗證(PoC)，以驗證整個解決方案的可行性。主要測試項目為虛擬化功能、是否與目前的員工帳戶直接結合、不必變動，對內對外的上網是否順利，以及與第三方CDR整合時的檔案清洗效果和速度。由於與週邊設備整合的客製化需求以及檔案清洗功能等效益最能符合期望，Citrix Virtual Apps and Desktops (虛擬應用程式與桌面) 解決方案獲得了第一銀行的青睞，並由彙典科技協助執行。

Citrix 方案只需六分之一的伺服器

在概念驗證評選的過程中，第一銀行還發現了部署成本的巨大節省效益。Citrix Virtual Apps and Desktops 的設計架構不同於其他競爭對手，其安裝的每一台虛擬上網主機都不需要硬碟，因此占用極少的硬體資源，因此第一銀行整個虛擬上網環境只要四台伺服器就可以滿足 7,000 人高速上網，而大部分競爭廠商的解決方案需要約 26 台主機才能支援。

在經過為期一年，三個分行、總行三個單位的試行 (Pilot Run)，逐步、分批立即解決各種狀況後，2019 年 8 月台灣所有分行全線導入。「導入 Citrix Virtual Apps and Desktops 所獲得的最主要成效，第一個就是員工有了一個安全的上網環境，第二個則是員工作業電腦直接對外的連網途徑被阻絕，讓駭客無法遙控，從資安的角度，這就是非常重大的成效。」張晉榮表示。

Citrix 此種虛擬上網的功能，來自其雙網隔離的概念，也就是當員工從公司外部存取公司內部資源時，資料不存放在員工的電腦中，可避免發生資料外洩事件；當員工需要從公司內部網路存取外部資源時，因為只有虛擬平台是對外的，所以就算駭客從郵件或者其他管道入侵員工電腦，放置惡意程式或勒索軟體，也無法遙控員工的個人電腦或發動勒索軟體。

在管理方面，由於不論是更換平台或應用程式，因為都集中在虛擬化環境中進行，所以除了員工不會受到任何影響、感覺不到有何操作差異性之外，後續的系統維護工作也很簡易。

防毒軟體警示數量從 100 降至 0

同時，另一個明顯成效則是系統中的防毒軟體不再發出警示 (Alert) 了。

過去同仁上網、下載檔案時，個人電腦中的防毒軟體每個月大概會偵測並發出一百多個惡意程式警訊。但在部署Citrix Virtual Apps and Desktops 虛擬上網平台，並整合第三方的 CDR 資料清洗軟體後，所有可能的惡意程式都在虛擬平台中被清洗，無法進入員工的作業電腦，所以防毒軟體再也不會發出警示。這種從一百到零個的警示成效非常顯著。

第一銀行能夠領先台灣金融業界，第一個成功完成全行虛擬上網的資安專案，除了優異的解決方案及廠商協助之外，張晉榮指出，在審慎評估、勇於任事之外，公司高層的支持與完善的事先準備都是重要的成功因素。

由於此一專案前所未有、技術嶄新、投資金額高，且導入過程中無論如何無縫接軌，總是對工作方式有一點影響，使用者可能會有少許反彈，必然需要高層在預算上的鼎力支持與協助宣導，才能順利推展下去。同時，完整的概念驗證與試行計畫等事前準備，也提高了專案的成功機率。

展望未來，因應此次新冠疫情 (COVID-19) 而產生的居家辦公需求，第一銀行也將與 Citrix 探索讓數千名員工透過虛擬平台安全連線與作業的資安新任務，但完整的測試與確保轉換流程的順暢 (smoothly) 仍是第一銀行執行資安專案不變的精神。

citrix

台灣思杰系統股份有限公司

台北市信義區 110 信義路五段 7 號台北 101 大樓 57 樓
郵遞區號：110
電話：008 0161 1351
傳真：+886 2 8758 2999
電郵：taiwaninfo@citrix.com