



IT 應使用門禁控制物理設施的 5 大理由

白皮書

選擇一種易於 IT 部門和使用者使用的建築物保全系統指南

網路安全與建築物保全同樣重要。無論對任一種系統妥協讓步，組織將立即暴露於危險之中。雖然目前許多網路安全系統的設計都支援 IT 最佳實務與標準，但是如虛擬化、物理門禁控制系統 (PACS) 的傳統設計並沒有考慮到 IT 專業人員。

這些舊有系統不只讓 IT 部門更難以進行部署、支援與維護，也成為實體安全與設施操作人員管理日常事務時的繁重工作，而且常需要昂貴的獨立伺服器、個別授權的軟體和專有的門禁硬體，同時只能從少數獨立的辦公電腦存取。

幸運的是，這些限制最終發生改變，作為經濟實惠的新一代門禁系統，以網路為基礎的物理門禁控制系統具有超越傳統 PACS 系統的多項關鍵優勢。雖然有許多因素需要考慮，但是一種 IT 化且介面易於使用的物理門禁控制系統，應具有的最重要五大特性，包括：平台可靠性、系統安全性、移動存取性、易用性和非專用門禁硬體。

本指南的編寫目的是協助 IT 專業人員評估其現有建築物保全系統的有效性，並與其物理安全系統同事共同找到一種可滿足組織整體安全性、IT 和預算需求的物理門禁控制系統。



1. 可靠性

確保門口按要求即時打開或關閉，可能看似很簡單，但花時間確保物理門禁控制系統的可信和可靠是不可少的。這不僅僅是指試用、調適或變換期間對 PACS 的故障排除和測試，還包括軟體平台和產品本身基礎系統架構實際設計的轉換。

傳統的物理門禁控制系統常需要在每處設施都部署一台獨立的 Windows 伺服器，這不僅增加維護和授權成本，還會造成單點故障。伺服器發生故障停機時，門禁控制器和讀卡機只能對那些在現場本機儲存的身份進行授權，而無法更新身份、許可權和原則，直至伺服器得以維護或修復為止。

下一代 PACS 可以簡化系統冗餘，提供具成本效益的自動容錯移轉和熱待命功能，尤其是作為價格實惠的全功能型門禁控制網路設備或固態機架式伺服器提供時。不用再購買昂貴的獨立伺服器，組織可以部署兩台或更多台可在所有設施和門禁控制器之間即時同步身份、角色和原則的網路設施，以降低成本並提高安全性。

藉由部署可在虛擬伺服器環境中執行的 PACS，IT 專業人員可以進一步降低成本、提高擴充性和改善可靠性。在虛擬伺服器中執行的系統可以快速完成設定，將硬體成本降到最低，容錯移轉的處理也更輕鬆。容錯移轉虛擬機器 (VM) 可以自動佈建並實行，同時在不中斷服務的情況下修復現有的 VM 部署。

虛擬化實體安全設施的 5 大理由

- 1 無需支付獨立伺服器的成本
- 2 在私有雲端中管理建築物保全系統
- 3 善用虛擬伺服器基礎架構
- 4 將停機時間降到最低，發揮最大的可靠性
- 5 減少設置與部署的時間

2. 安全性

過去，大多數的建築物保全系統一直專門由具有實體安全行業背景的製造商製造。為了讓建築物管理員高枕無憂，這些開發人員往往傾向囊括所有必要的重要功能，但除非 IT 專業人員的物理門禁控制系統接受全面的代碼檢查，否則失眠的可能是這些 IT 專業人員。尋找的平台應具有某種保證，如獲得業界公認的 PACS，從而確認其應用程式能夠抵禦已知的軟體漏洞，以降低或消除網路攻擊的風險。

不只軟體弱點會造成疑慮，也需要考慮到作業系統和伺服器弱點。例如，許多舊有的物理門禁控制系統的設計是執行於標準應用程式或資料庫伺服器上，這通常需要不斷的弱點修補和持續的 IT 資源，以確保系統連接網路時，不會暴露在最新的安全性威脅下。

數家製造商已經開始提供 Linux 基礎的 PACS 平台，其大量減少了系統設置、支援與維護問題，同時消除了修補管理和安全性的頭疼問題。使用者將透過精簡型用戶端的網路瀏覽器 (而不是厚重型用戶端的應用程式) 嚴格進行控制，安全、開放原始碼且基於 Linux 的物理門禁控制系統也許可以提供您在建築物保全系統中尋覓的那份放心。

3. 移動性

行動運算的崛起是難以忽視的，Forrester Research 公司在 2012 年一份研究中指出，將近 60% 的公司員工會在辦公室以外的地方透過行動裝置分享、存取和管理內容。有鑒於行動需求不斷增加，選擇以網路為基礎的物理門禁控制平台時，若所處位置能存取網路，使用者將可從網路瀏覽器管理建築物保全系統。

傳統上基於軟體的 PACS 只能在特定的桌上型或筆記型電腦上運作，迫使 IT 部門安裝和/或升級獨立授權的軟體和一次一台的伺服器。舊有系統也會把設施管理員和保全主管束縛在辦公桌前，無法從遠端進行工作。

管理設施時需要人員每天親自進行大量監控，因此尋找一種既能在各種行動裝置上運作，又能在各種 PC 和 Mac 網路瀏覽器 (像是位於建築物地下室的桌上型電腦) 上運作的物理門禁控制系統便十分重要。

運用以網路為基礎的門禁控制系統，設施管理員可以帶著智慧型手機或平板電腦到公司外的會議場地或建築物的頂樓，而仍然可以回應警報、變更門禁排程或檢視視訊監視片段。IT 專業人員、系統整合商和保全廠商也可以從任何網路瀏覽器登入系統來變更系統組態，或是持續提供支援。

另外，在具有多棟建築物、多個辦公室地點或異地園區的大型組織中，相較於僅依賴軟體的老舊厚重型用戶端模式，透過網路瀏覽器提供的精簡型用戶端系統架構將可在升級、管理與集中化設施門禁控制時，大幅降低成本及提高效率。除去額外的軟體與個別使用者授權成本，組織可以釋出他們的 IT 與保全預算，用於保護其他的門戶、建築或設施之上。

行動化實體安全設施的 5 大理由

- 1 不需要安裝軟體或維護伺服器
- 2 從任何地方控制設施的門禁
- 3 隨時回應警報
- 4 不必再被綁在辦公桌前
- 5 使用您現有的行動裝置

4. 易用性

評估物理門禁控制平台的有效性時，容易使用是另一個重要的考量因素。雖然 IT 部門通常可以接受廣泛的軟體、硬體與使用者介面，但實體安全使用者可能並非如此熟悉使用進階電腦或管理複雜的作業系統。

前台保全巡邏人員或後台設施管理員應該能夠輕鬆地新增、刪除或調整門禁排程和使用者權限，不會感到系統令人望而生畏或使人不知所措。卡片、識別證和憑證的定期更新應該十分方便，以確保只有正確的人員可以存取正確的房間和資源，以前的員工再也不能進入建築物。而且，警報還應該能夠從各種視訊監視平台輕鬆地查看並相容，為實體安全團隊提供所需的資訊，以便他們迅速調查系統警報、安全違規或原則違規。

另一方面，IT 專業人員更喜歡按照他們的工作方式建立的系統，其設計可與標準 IT 系統相整合。例如，支援輕量型目錄存取通訊協定 (LDAP) 的平台能夠與組織現有 HR 員工資料庫、Active Directory 或身份存取管理 (IAM) 系統繫結，而無須再維護兩套員工和訪客身份，甚至允許組織對網路門禁控制系統中現有的使用者分配建築物存取權限。另外，某些物理門禁控制系統還能夠輕鬆地將建築物保全資料整合到安全資訊與事件管理 (SIEM) 系統中，讓組織獲得整個企業的統一安全系統檢視。

現實世界的接壤

如果伺服器房間的門被撐住打開，完全整合的系統將傳送警示至實體安全的相關人員，讓他們可以立即切換到視訊播放即時監控發生的情況。系統將自動暫停鄰近房間的網路存取，直到 IT 與實體安全人員檢閱 SIEM 記錄檔查明發生或未發生的情況，輕鬆存取門口周圍的所有活動，包括最後刷卡進入的人。正確的門禁控制平台可讓所有人的工作更輕鬆，最終降低小意外失控釀成大禍的風險。

5. 靈活性

無論您是需要保護一個站點中的幾個房間，還是多個建築物和辦公地點中成千上百個的房間，物理門禁控制系統都可以隨著組織的規模而擴充，這是非常重要的。

由於門禁硬體佔了物理門禁控制系統很大一部分的成本，包括安裝在建築物牆壁與天花板上的控制器、交換器與讀卡機，因此務必選擇基於開放、非專有門禁硬體的門禁控制系統，好為您的組織提供最大的靈活性。

許多物理門禁控制系統都仰賴只能使用單一物理門禁控制系統的專用門禁控制器和讀卡機，因此將組織局限在只能與單一的製造商、系統整合商和軟體平台進行交易。如果您對系統、升級成本或廠商的支援水準不滿意，更換設施的成本將遠遠超過部署新系統的成本。

開放型架構系統允許 IT 和實體安全團隊充分利用其在可重複使用的非專用門禁硬體上的投資，使他們只需採購新的前端系統，無須購買和安裝全新的門禁硬體和控制器，從而更輕鬆、更經濟地升級門禁控制系統。由此，其 IT 和保全預算可以使用更長時間，不需要被迫使用已經整合到專有門禁硬體上的軟體平台。隨著組織規模的擴大或門口數量的增加，IT 部門只需新增更多非專用硬體，而不必擔心硬體投資的過時問題。

而且，由於不斷發展的門禁控制系統業務仍然存在激烈的競爭，製造商和廠商不能掉以輕心。

避免使用專有門禁硬體的 5 大理由

- 1 軟體與廠商受限
- 2 製造商與廠商因此感覺自滿
- 3 成本支援與維護規劃
- 4 過高的更換設施成本
- 5 投資遠景不明

概要

IT 需要的開放式架構系統應提供更好的擴充性、虛擬環境安裝選項，以及與其他 IT 和實體安全系統整合的改進選項。這些技術不僅需要易於部署，例如部署在虛擬伺服器環境中，還需要系統能夠抵抗網路攻擊，同時保持完全可靠。

同時，設施團隊需要的是一種使他們的生活更輕鬆的解決方案。他們希望此方案能夠輕鬆地變更、新增或刪除系統使用者，而且需要支援靈活性，當發生情況時允許存取異常情況，還希望無論他們置身在建築物何處，都能使用智慧型手機或行動裝置控制門禁授權，不必再束縛於辦公桌前。

一個滿足所有人需求的系統不僅能改善工作流程，還可以降低開支，無論現在或未來皆然。組織若能覓得在門禁控制之外，同時提供視訊監視、身份管理與 SIEM 的系統，便能更高效並有智慧地掌握所有情況。

但最重要的是，這樣的系統打破了長久以來阻隔物理與邏輯門禁控制系統結合的藩籬。IT 部門可以避免牽涉導致營運費用增加的不安全系統，更簡單直覺的使用者介面也可以縮短設施人員的培訓時間。一旦獲得一種易於 IT 部門和使用者使用的建築物保全系統，這兩方終於可以互相合作，變得更有效率，同時消除流程中的安全漏洞。

