白皮書 – **2018 年 3 月**

全方位的數位工作區安全性方法

vmware®

目錄

有些公司為員工提供想要和需要的應用程式，並讓他們可以隨時隨地透過任何裝置存取這些應用程式，藉此強化員工的工作能力；不論是個人還是組織層面，這些公司都能因此在決策、生產力與工作效率上獲得可具體衡量的效益。[1]

簡介

全新量化的商業效益顯示，當賦予員工數位工作區時，不但能夠提升其生產力，公司的績效也能超越傳統工作區，而這也讓企業更加注意如何安全地將應用程式交付到任何裝置上，同時達到類似的效益。每一家企業都想要獲得 Forbes Insights 在其《數位工作者的影響》(Impact of the Digital Workforce) 研究報告中所提出的優勢，但是即便如此，也不應該犧牲安全性來達到目標，尤其當傳統的工作疆界日益模糊時更是如此。

日趨模糊的工作疆界，讓企業組織的曝險程度增加

各地區的 IT 團隊持續對抗數量與嚴重性雙雙不斷增加的安全性威脅。對許多企業來說，惡意軟體入侵已經導致其面臨成本昂貴的營運中斷。舉例來說，WannaCry 網路攻擊就利用了 Microsoft Windows 的漏洞來鎖定數以百萬計的電腦發動攻擊，同時間掌控 150 個國家/地區的電腦，並以之交換勒索贖金。在美國，2017 年追蹤到的資料外洩事件數量達到歷史新高。[2]

時至今日，不斷拓展的組織與工作疆界，為網路罪犯提供了更加有利的商機。其中有名的例子為現代零時差威脅及中間人 (MITM) 攻擊，前者以攻擊時間來命名，因為攻擊行為通常發生在開發人員察覺這項程式錯誤的前一天或第一天 (或「第零天」)；而後者則是一種監聽形式，攻擊者會主動監聽及攔截公開金鑰的訊息交換並重新傳輸訊息，同時以自己的金鑰來取代要求的金鑰，進而在幕後默默地接管、監控及修改兩位使用者之間的通訊內容而不被察覺。[3] 利用社交工程與程式設計專業能力、殭屍網路與勒索軟體威脅的進階網路釣魚技巧，讓企業組織更容易暴露在風險之中，即便企業組織事先有所準備仍舊是防不勝防。

對抗各種威脅並保護企業資料

確保不斷演進的數位工作區安全，較好的方法是透過智慧型平台來防護、偵測與補救各項威脅。有了這個方法，當動態網路威脅態勢不斷加劇並調整以鎖定傳統工作疆界以外的全新弱點而發動攻擊時，企業組織的數位工作區策略就能持續擴充與進化，以便更有效地保護敏感資料。

本白皮書說明一項全新的全方位可預測安全性方法，可在工作疆界日趨模糊的當代世界中提供保護。內容強調確保不斷演進的數位工作區安全的重要性，並指出企業需要在商業網路的各項元件間導入信賴架構。另外，此白皮書還介紹了關於防護、偵測與補救的八大核心功能，以確保 IT 部門能夠從收集到的資料當中獲取深入見解並加以運用，以做出有利於防範威脅並阻止攻擊行為不斷擴散的決策。

---

1 Forbes Insights，《高績效數位文化：賦能、信賴，乃至於員工與 IT 之間的全新平衡》(The High-Performance Digital Culture: Empowerment, Trust, and the New Equilibrium Between the Employee and IT)，2017 年 10 月。

2 Identity Theft Resource Center，《2017 年度資料外洩事件回顧》(2017 Annual Data Breach Year-End Review)。

3 3 Technopedia，《零時差威脅》(Zero-Day Threat)，2018 年。

「安全性是 2018 年行動化與數位工作區投資的優先要務」。

– CCS INSIGHTS 公司

安全性是企業推動現代化數位工作區策略的最大阻礙

在現今的時代，隨時隨地辦公已經不是新鮮事。不管是在辦公室、家中、咖啡廳，甚至在一萬英尺高空，員工隨時隨地可以透過各種網路，存取位於個人與企業端點的資訊與應用程式。IT 團隊體認到員工對於時間、地點與所使用的工作裝置需要更靈活的選擇權，因此正試圖在確保珍貴的企業資料安全之際，滿足員工的偏好。

只不過現有的安全性解決方案仍舊不敷使用。IT 團隊仍在嘗試使用由各種傳統安全性技術所拼湊出來的複雜方案，來應付快速變化的使用者需求，其中有些技術甚至是勉強部署出來的，至於能不能保障安全則一點把握也沒有。隨著 IT 團隊陸續採購多項功能不同的解決方案，許多技術彼此之間並無法順利溝通協調，而這也為有心人士提供了多種潛在的攻擊可能。雖然員工的滿意度攸關企業組織的成功與否，但 IT 主管們紛紛回報安全性是 2018 年行動化與數位工作區投資的優先要務。[4]

近期由 CCS Insights 公司所進行的一項調查中顯示，將近一半 (47%) 的 IT 買家表示網路安全性是他們接下來 12 個月要針對數位工作區優先投資的標的，第二順位則是裝置安全性 (42%)，而應用程式安全性則位居第三 (27%)。這些投資項目能夠隨著工作負載遷移為資料與應用程式提供更安全的防護能力；然而，安全性解決方案資訊孤島的存在，只會增加複雜度，進而留下犯錯空間。舉例來說，儘管企業一直透過網路防火牆防止入侵行為滲透到系統當中，但是後來才發現該入侵行為已經感染了各種系統的東西向流量，持續數個月而未偵測出來，這對企業造成了嚴重危害。當 IT 依據信賴架構串連各自為政的安全性解決方案資訊孤島時，就不需要在防護、偵測與補救威脅上排定優先順序，因為這項信賴機制已經默默地持續協調執行這三大功能。

透過現代化數位工作區安全性做法，企業能夠更有效地對抗不斷演進並鎖定系統與資料發動攻擊的網路威脅，讓員工的數位工作區隨時獲得所需的安全性。這項做法必須在各項元件之間建立信賴關係，確保包括員工、應用程式、端點與網路在內的終端使用者運算商業網路安全，而且僅允許通過驗證的授權存取行為。整合的全方位信賴架構有助於確保資料獲得保護，並可透過洞悉力和自動化智慧功能，用於持續偵測並補救威脅以有效將風險降至最低。

4 CCS Insights 問卷調查，《IT 買家調查》(IT Buyer Survey)，2017 年 9 月。

全新安全性需求

- 為了確保企業組織的安全性，請採用關於防護、偵測與補救的八大核心功能。
- 為了取得彙總檢視，需要運用架構來建立保護商業網路的各項元件之間的信賴關係。
- 為了持續緩解風險，企業需要從環境中取得洞悉力，以便採取防範未然的自動化決策方針，確保數位工作區安全無虞。

面對不斷演進的數位工作區，推動全方位安全性的三個步驟

IT 部門需要全面的企業安全性方法，以保護其使用者環境的安全。此模式銜接了安全性技術資訊孤島，因此涵蓋了端點、應用程式、員工與網路的安全性。為獲得最佳成果，IT 必須將這些步驟納入考量，以便有策略地保障其不斷進化的數位工作區安全。

步驟 1：防護、偵測與補救威脅

網路威脅不斷地進化。一開始只是無傷大雅的入侵活動，現在幾乎成為帶有不法意圖的駭客行為，例如學生為了向朋友炫耀其 IT 能力，在未經授權的情況下入侵然後立即離開系統的行為。防範網路犯罪，需要一套完善的回應機制，以便在保護好人之際同時驅逐壞人，進而：

防護

企業 (尤其是金融服務與醫療保健等受到監管的企業組織) 繞了一大圈終於讓存放高機密與珍貴資料的後端儲存裝置符合合規要求。然而現今的客戶經理可能會在客戶會議期間透過行動裝置存取敏感資料，然後不小心將平板電腦留在計程車上，導致敏感資料可能遭竊。這些失竊並遭到盜用的客戶資訊，到最後幾乎毫無意外地為品牌形象與財務帶來負面影響。

讓員工得以輕鬆存取消費者資料及應用程式的能力，不應該為公司帶來極大的風險。因此，企業安全性部門開始保護員工的數位工作區安全。IT 必須教育員工不要點選可疑的連結，同時藉由部署安全原則來防範資料遺失，以防範惡意軟體入侵環境。當企業組織能夠全盤掌控從員工與應用程式到裝置與網路的所有資產狀況，就能進一步識別弱點並保護環境免於內部與外部的雙重威脅。只有當企業組織充分實作各種防護措施，包括發佈存取控制、敏感資料分類與裝置使用限制等原則，乃至於定期修補應用程式時，才能放心地推進到偵測階段。總之，如果只有防護措施而沒有同樣有效的偵測方法時，IT 便無法得知是否真正解決了最重要的問題。

偵測

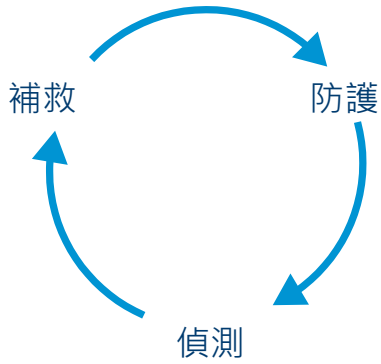
日益模糊的工作疆界、內部威脅與技術持續精進的網路罪犯，讓安全性對話重點從攻擊「是否會」發生變成了「何時會」發生。因此，企業不僅要保護資產，還必須進一步在入侵行為發生之際偵測威脅，包括認證遭到入侵，乃至於未套用修補程式的系統漏洞遭到利用。IT 團隊必須有能力識別並消除主動威脅，阻止其對企業組織造成進一步的傷害。實作偵測措施時，不能因此觸發過多的警示通知而產生狼來了效應。

當威脅入侵數位工作區時，做好準備的企業可透過持續運作的自調式監控功能加以偵測，讓 IT 部門與安全團隊得以找到位於行動與桌面平台端點和應用程式上的威脅。透過自動化的持續監控與警示功能，隨時掌握存取資訊的人員、存取內容、地點、方式與媒介網路，IT 便能有效掌控一切。接著，透過最後已知的良好狀態、記錄功能，以及透過分析技術所呈現的智慧功能，IT 便擁有所需的工具能夠識別可疑的行為，並利用這項洞悉力做出有利於後續作業的最佳決策。

補救

數位企業步調快速，對於大多數工作而言，需要人工作業進行補救的傳統安全性解決方案已經無法滿足需要。今日的企業需要快速的回應機制，以便處理惡意入侵與非預期的營運中斷事件。等候回應的這段期間，可能會出現更重大的資料外洩事件。VMware 的一份內部報告指出，1/10 的企業客戶需要一年以上的時間，才能實作完成影響其大部分，甚至是全部端點的所有 Windows 系統修補程式。而網路安全罪犯就可利用這段安全性空窗期間，發明更多的攻擊手法。

IT 團隊必須有能力利用從環境中獲得的洞悉力，依據根本原因信心十足地預先定義各項原則，以便快速自動回應問題並復原系統，讓營運重回軌道。透過自動化機制，IT 可以選擇隔離、暫停或是封鎖應用程式或雲端服務的存取。偵測到威脅後，準備最充分的企業就能利用有效的解決方案，並透過引擎偵測行為異常以自動執行補救措施，同時啟動自動化原則以封鎖敏感資料的存取。



當企業選擇以策略性架構，來建立其商業網路中各向元件與保護這些元件的解決方案之間的信賴關係時，能夠確保在最佳狀態下充分保護重要的企業資產，並加速威脅偵測與補救的時間。

步驟 2：防護、偵測與補救的能力

這八大關鍵功能協助企業朝著現代化的全方位數位工作區安全性邁進：

單一開放平台方法	單一開放平台讓 IT 得以簡化合規措施 (例如對裝置與應用程式的規定)，並減少風險。企業應該採用結合存取、裝置與應用程式管理功能，並搭配分析及智慧技術的單一開放平台，才能以獨家技術銜接複雜且成本高昂的現有安全性解決方案資訊孤島。具備智慧服務的平台可確保工作區資料得以彙總、相互關聯並提供各項建議，賦予整合的洞悉力與自動化功能。 使用這項方法的企業能夠對所屬員工、應用程式、端點與網路獲得彙總檢視能力。此平台技術必須建立在 API 通訊架構上，以協助建立企業商業網路中各項元件之間的信賴關係。這點很重要，因為當整個數位工作區的信賴關係建立之後，員工便能透過彼此互連且權限降至最低的系統輕鬆取得所需的功能，同時確保具備安全性。
資料外洩防護 (DLP) 原則	資料外洩防護 (DLP) 原則可協助企業組織保護位於任何一處的資料安全，無論其位於資料中心內外皆然。IT 團隊應該要能遠端鎖定遺失或遭竊的裝置或是清除其內容、定位遺失的裝置，以及取得即時的裝置資訊 (例如作業系統 (OS) 版本、最新更新、位置等)。使用虛擬桌面基礎架構 (VDI) 來集中管理桌面平台與應用程式，可以減少遺失或失竊裝置的資料損失。 針對所有端點，企業應該要能運用原生作業系統所提供的資料外洩防護 (DLP) 控制功能，對個別應用程式實施及管理安全性原則，並透過電子郵件附件控制、剪下/複製/貼上限制，以及動態浮水印效果等功能來防止內容出現資料遺失。透過軟體開發套件 (SDK) 控制及限制使用者移除來自企業的內容，是必要的措施。 原則與合規引擎可協助自動確保進階資料外洩防護 (DLP) 的合規性。進階安全性原則包括針對具有根存取權限或遭破解裝置設定的保護措施、設定白名單和封鎖清單的應用程式、限定開啟環境的應用程式限制、地理位置限制、網路設定、封鎖匯出與螢幕擷取作業，以及將公司資訊備份或儲存到外接 SD 記憶卡或遠端雲端備份解決方案
關聯性原則	使用關聯性原則來設定並實施有條件的使用者存取，可協助確保只有授權的使用者能夠存取敏感資訊與資源。企業必須有能力依據角色、部門、放行等級建立條件式存取，這樣唯有授權的使用者才能存取到特定的資訊與資源。 透過原則施行與存取及裝置管理機制的搭配運用，IT 就能限制資料、應用程式或裝置的使用者權限。同樣的技術也可用於將條件式存取套用到行動應用程式上，確保唯有符合標準的應用程式能夠存取內部系統。

保護應用程式	只要在應用程式層級實施資料外洩防護 (DLP) 原則，企業就能邁開大步，用更精細的存取原則提供更完善的資料保護。數位工作區應該納入資料外洩防護 (DLP) 原則 (已於先前的第二項功能說明中介紹)，以提供和應用程式層級一樣的功能。 對於用戶自攜裝置 (BYO) 與企業裝置來說，行動應用程式管理機制有助於提供佈建與控制存取，實際上還能透過依身分識別定義的原則來保護應用程式。同理，雲端資料遺失保護，乃至於管理已批准及未批准之雲端服務的存取與活動，能更有效地保護資料並抵禦各項威脅。 透過支援完整裝置 VPN、個別應用程式 VPN，以及針對各大作業系統 (包括 iOS、Android、macOS 與 Windows 10) 進行採用 SDK 的 Proxy 閘道通訊作業，IT 能夠彈性地選擇適當的解決方案，以確保應用程式連線能力。 此外，生產力應用程式 (例如電子郵件、文件管理等) 必須提供資料外洩防護 (DLP) 與權限管理服務 (RMS) 功能，包括： • 透過資訊權限管理 (IRM) 保護的電子郵件 • S/MIME 與 PKI • 電子郵件分類 • 敏感或個人身分識別資訊 (PII) 原則 • 附件加密 • 列印、檢視與漫遊的存取原則 • 文件到期 • 浮水印效果
存取管理	企業透過多重因素確認使用者身分，或是一次針對許多應用程式確認其使用者身分，以強化資料保護。由於應用程式、裝置與雲端服務數量越來越多，如果每次都要個別設定原則，程序會變得相當繁瑣，為此，企業應該要利用使用者身分來建立安全性參數。 一鍵式單一登入 (SSO) 可讓使用者存取桌面平台、行動與雲端應用程式，省下多重登入所花費的時間和麻煩。透過 SSO，就能同時針對多個應用程式確認使用者身分，猶如提供使用者一把開啟單一數位工作區的鑰匙，方便其從應用程式目錄中，存取位於自選端點上的各式各樣 Web、行動、SaaS 與舊版應用程式。 有了多重要素驗證 (MFA) 機制，使用者和系統元件的身分就可透過多重因素 (而非單一密碼) 進行確認，並對應至所要求的存取或功能的連帶風險。
加密	加密機制可防範非指定收件人在敏感資料傳送期間肆意查看，讓企業組織可以確認其資料受到保護。在關鍵業務流程方面，最佳做法包括在儲存或傳送時加密所有資料。萬一資料外洩，被竊取的關鍵檔案也應只是無法判讀的資料而已。針對傳輸中資料與靜態資料使用 AES-256 位元加密等進階加密標準，是相當重要的做法。 作為裝置平台與企業系統之間的中繼點，IT 可以運用通道或是個別應用程式 VPN 以及使用獨特的憑證，驗證與加密個別應用程式 (位於符合標準的裝置上) 通往其想要進行存取之後端系統的流量。

微分段	企業組織可以在整個網路上實作微分段，更積極地抵禦威脅、降低風險並提升安全態勢。微分段可提供各項功能組合，包含： • 透過分散式具連線狀態防火牆與 ALG (應用程式層級閘道)，且精密度以工作負載為單位，以縮小資料中心周邊內的攻擊範圍 • 針對適用於虛擬機 (包括虛擬桌面與虛擬應用程式主機) 的物件型原則應用程式啟用安全性群組，以建立精密的應用程式層級控管機制 • 透過邏輯網路層疊式隔離與分段技術來橫跨機架或資料中心 (無須顧及底層網路硬體)，以利啟用集中管理式多資料中心安全性原則 整個 IT 環境分成幾個小部分，萬一某一部分遭到入侵時，才能更容易管理和保護，並抑制損害範圍。分隔資料中心裡從應用程式到特定工作負載之間的東西向流量，可大幅減少企圖對企業造成巨大損害的惡意軟體/病毒的攻擊媒介。
分析	企業可運用從應用程式部署及使用情況取得之可採取行動的深入見解，提升其安全態勢。IT 可透過彙總的應用程式部署、使用情況、裝置安全性與使用者經驗詳細資料，進一步瞭解其數位工作區環境的效能與安全性。內建的智慧服務，加上自動化行動，可加速規劃作業、強化安全性，同時提升使用者經驗。在工作疆界日趨模糊的今日，此舉還可持續監控安全性風險，並快速提出緩解回應。若與決策引擎一起使用，智慧服務有助於相互關聯各項資訊，以偵測威脅並透過存取原則自動執行補救措施。

步驟 3：信賴的合作夥伴部署安全的天羅地網

安全性威脅不論在發生頻率、衍生的成本，乃至於威力與精密度都有逐漸上升的態勢，為了抵禦、偵測與補救威脅，理想的做法是運用由信賴的安全合作夥伴廠商所組成的單一平台來實施無縫接軌的管理。獨立運作的舊式安全性工具雖然能夠保護貴重的資訊，但是 IT 人員卻無法充分掌握各項資訊，而且經常導致環境裡出現解決方案資訊孤島。這種彼此不協調的方法因為操作起來複雜繁瑣，而且需要人工作業來確保數位工作區的安全，對企業組織來說只是成本高昂的負面行為。

在為不斷成長與進化的數位工作區提供保護的各項元件之間建立信賴關係，有助於確保建構全方位的安全性。理想的做法是藉由建立在經驗證之數位工作區平台上的 API 來提供信賴架構。這是因為這些 API 讓豐富的安全性解決方案商業網路得以和平台本身進行溝通，最終讓管理員能夠透過想要和需要的彙總檢視簡化環境的安全性與管理作業。

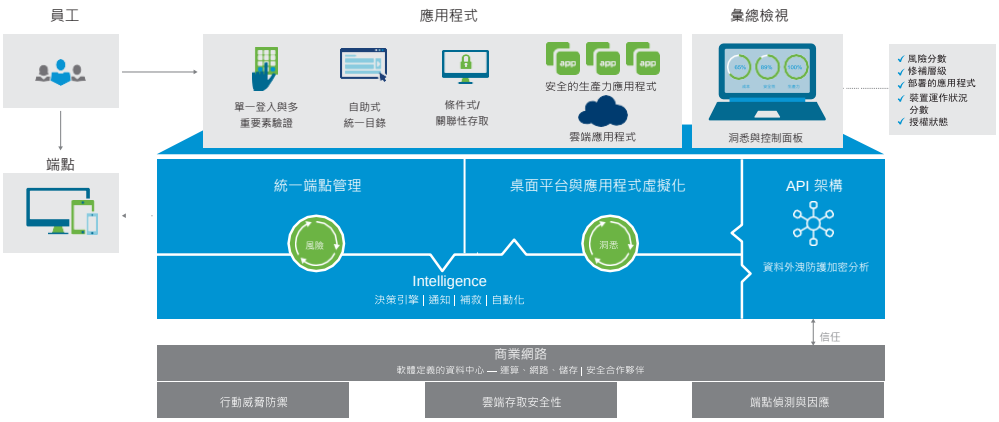
運作穩健的數位工作區策略包含由信賴的安全性解決方案所組成的開放式商業網路，有能力抵禦各項攻擊並緩解下列領域的風險：

- 作業系統安全性瑕疵能見度
- 裝置運作狀況評估
- 裝置復原
- 管理存取與控制
- 原則設定
- 病毒掃描
- 修補
- 災難復原
- 合規監控

VMware 如何協助傳統的數位工作區安全性脫胎換骨

儘管網路安全性工具的技術演進令人刮目相看，但是市面上的工具數量與種類，卻讓 IT 主管更加堅信數位工作區安全性的最佳實作方式尚未誕生。時至今日，企業可以自信地邁開大步，在不斷變遷的網路威脅態勢下運用 VMware 所提供的技術架構對抗各種攻擊，進而簡化安全性管理作業。

VMware® Workspace ONE™ Trust Network™ 為您企業內的員工、應用程式、端點及網路提供全面且現代化的企業安全性。Workspace ONE Trust Network 所提供的一系列功能可依據信賴架構與驗證機制，保護整個不斷進化的數位工作區，偵測其中的威脅，並進行補救。當整個數位工作區的信賴關係建立之後，員工便能透過彼此互連且權限降至最低的系統輕鬆取得所需的功能，同時確保具備安全性。為了管理與當代網路威脅相關的風險，Workspace ONE Trust Network 結合來自智慧型數位工作區平台 Workspace ONE 的洞悉力與信賴的安全合作夥伴解決方案，共同為數位工作區提供可預測的自動化安全性機制。



防護、偵測與補救

VMware 所採行的方式有助您的 IT 營運與安全團隊簡化安全性功能 (例如使用 NIST Cybersecurity Framework 等架構) 與 Workspace ONE Trust Network 方式所提供的解決方案功能之間的對應關係，進而輕鬆管理網路安全性風險：

- 這些安全性功能首先會保護數位工作區，包括透過機器學習能力來辨識惡意軟體、實作網路微分段技術來防範進階的持續性威脅 (APT)，並防止資料從企業雲端式應用程式中非法外洩。
- 隨著各式威脅入侵數位工作區，VMware 安全性功能可透過持續運作的自調式監控功能，偵測整個行動與桌面平台端點及應用程式上的威脅。
- 這個方法會接著運用強大的決策引擎自動補救。例如，當系統依據行為異常指標偵測到特洛伊木馬或 MITM 攻擊行為時，會利用自動化原則來封鎖企業資料的存取。

運用分析技術統一存取、裝置與應用程式管理作業

Workspace ONE Trust Network 結合了 Workspace ONE 數位工作區的核心功能 (包括存取、裝置與應用程式管理)，以及 Workspace ONE Intelligence 所提供的分析能力，以獨家技術銜接現有的安全性解決方案資訊孤島。Workspace ONE Intelligence 服務可確保工作區資料得以彙總、相互關聯並提供各項建議，賦予整合的洞悉力與自動化功能。VMware 藉由 Workspace ONE Intelligence 服務來提升 Workspace ONE Trust Network 功能，確保企業組織能夠針對工作疆界日趨模糊的今日企業環境，持續監控安全性風險並快速提出緩解回應。

決策引擎有助於相互關聯各項資訊，例如將不在網路內的企業裝置與使用者行為關聯，以偵測各項威脅並透過存取原則自動實施補救措施。運用整合式洞悉力探查威脅資料，同時透過精密裝置合規狀態，可輕鬆地即時識別並緩解安全性問題，改善數位工作區的安全性運作狀況。透過決策引擎，IT 能建立各項規則以自動化及最佳化常態性工作，例如使用重要的修補程式來補救脆弱的 Windows 10 端點，並在群組或個別層級設定應用程式與服務的條件式存取控制。

善用信賴的合作夥伴解決方案商業網路

若要對整個數位工作區貫徹全面的安全性，必須在為不斷成長與進化的數位工作區提供保護的各項元件之間建立信賴關係。VMware 為達到這個目的，運用 Workspace ONE Trust Network 並充分善用建立在 Workspace ONE 平台上的 API 來提供信賴架構。這些 API 有助於確保豐富的安全性解決方案商業網路得以和 Workspace ONE 進行溝通，最終讓管理員能夠透過所需的彙總檢視簡化環境的安全性與管理作業。

藉由串連安全性解決方案資訊孤島，VMware 客戶便可有效運用現有的技術投資，大幅提升持續監控與風險分析效能以加速回應時間，並依據各項趨勢及可隨部署擴充的運作模式建立一套可預測的安全性策略。

VMware 客戶可有效運用現有的技術投資，大幅提升持續監控與風險分析效能以加速回應時間，並依據各項趨勢及可隨部署擴充的運作模式建立一套可預測的安全性策略。

由於工作場域的疆界日趨模糊，企業有必要採用全新的數位工作區安全性做法。在商業網路中的各項元件之間建立信賴架構，以滿足新員工、新應用程式、新裝置及新網路的需要。有了這項架構作為技術基礎，數位化企業就能大步向前，同時緩解各項風險、保護品牌商譽、降低營運成本、提升靈活性，並針對工作上的所有裝置提供類消費者經驗。

防護、偵測與補救：8 項必備能力

vmware WORKSPACE ONE™ TRUST NETWORK

功能	重要性
單一開放平台做法	消除遍及各平台、應用程式與使用者設定檔的技術資訊孤島，進而簡化合規措施並降低風險。
資料外洩防護 (DLP) 原則	透過裝置清除、遠端鎖定與個別應用程式安全性原則，保護位於各處的資料。
關聯性原則	施行條件式存取原則，確保只有授權的使用者能夠存取敏感資訊與資源。
保護應用程式	在應用程式層級上實施資料外洩防護 (DLP) 原則，控制可存取特定資源的人員，達到保護資訊安全的目的。
存取管理	透過多重因素確認使用者身分，或是使用單一登入一次針對許多應用程式確認其使用者身分，以強化資料保護。
加密	防範非指定收件人在敏感資料傳送期間肆意查看，確保敏感資料的安全。
微分段	藉由區隔工作負載與流量，縮小企業組織所面臨的攻擊範圍。
分析	透過可採取行動的洞悉力、應用程式分析與自動化功能，提升安全態勢與合規性。

深入瞭解

賦予員工數位工作區以強化其工作能力，可進一步嘉惠工作人員及企業。千萬別因為 IT 安全性考量，而犧牲了生產力與效率優勢。由於您的數位工作區策略會隨著機動性極高的網路威脅不斷地擴張及進化，而這些威脅隨時可能升高攻擊強度並自我調整以鎖定傳統工作疆界以外的全新弱點發動攻擊，因此貴企業有必要採用 Workspace ONE Trust Network 技術以獲得所需能力，確保具有全方位安全性以保護敏感資料的安全。您可以結合運用存取、裝置、應用程式管理與分析技術來保障數位工作區安全，為整個商業網路建立信賴架構，同時從收集來的資料當中擷取深入見解並加以運用，以做出合適的安全性決策。

深入瞭解 Workspace ONE Trust Network：www.vmware.com/tw/products/workspace-one/security。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
台北市 110 信義路五段七號台北 101 大樓 57 樓 C 室 電話 +886-2-8758-2804 傳真 +886-2-8758-2708 www.vmware.com/tw

文件編號：VMW-WP-CMPRHENSIVE_APPROACH_SECURITY_WRKPLC-A4_103