管理您的
老舊作業系統

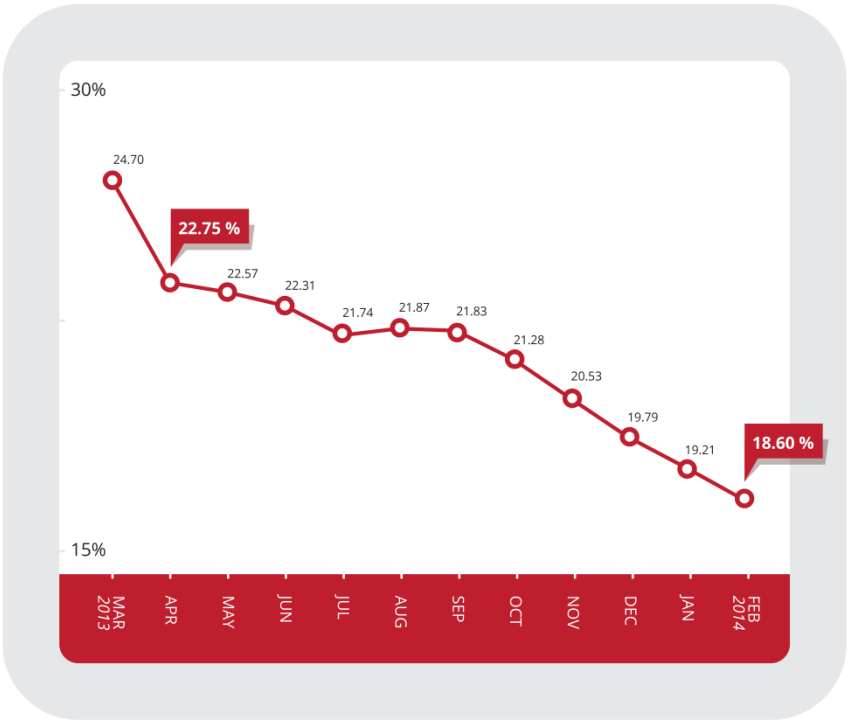
Windows XP 終止支援之後
未來的日子將變得如何？

Microsoft 長達十多年的 Windows® XP 支援即將在 2014 年 4 月 8 日劃下句點。使用者再也不會收到安全更新、非安全相關修正，以及免費或付費的支援，同時線上技術資訊也不再更新。

支援終止即將到來，意味著仍在使用 Windows XP 的企業系統將面臨嚴重的後果。本文探討企業繼續使用這套作業系統所將面臨的威脅、潛在損失、法規遵循問題以及更高的使用者運算成本。

Windows XP 在今日作業系統市場的現況

圖一顯示 Windows XP 全球使用率在過去一年逐步下滑的趨勢。儘管該作業系統的市場占有率已經大幅滑落，但 Windows XP 在市場上仍占有一席之地。Microsoft 至今已雄霸用戶端作業系統市場長達二十多年。根據 IDC 的調查，每十台 PC 就有一台是使用 Windows 作業系統。[1] 此外，根據 Spiceworks 所作的一篇研究也發現，截至 2013 年 12 月為止，有 76% 的 IT 人員仍得支援 Windows XP 作業系統。其中，97% 支援的是桌上型電腦，68% 支援的是筆記型電腦。[2]



圖一：2013 年 3 月至 2014 年 2 月的 Windows XP 市場占有率。資料來源：StatCounter.com

1 Al Gillen、Randy Perry 與 Nancy Selig。(2012 年)。「降低風險：為何緊抓著 Windows XP 不放是件壞事」(Mitigating Risk: Why Sticking with Windows XP Is a Bad Idea.)。上次存取日期 2014 年 3 月 21 日：http://download.microsoft.com/download/2/2/A/22A70C6F-71F7-4984-8404- 4FBA665B27D8/WHITEPAPER%20--%20IDC%20MSFT%20-%20Migration%20from%20XP%20to%20Win7.pdf。

2 Spiceworks。(2013 年 12 月)。「該讓您的 XP 走了：Windows XP 支援終止以及為何難以分手」(Getting Over Your XP: Windows XP End-of-Life and Why Breaking Up Is Hard to Do.)。上次存取日期 2014 年 3 月 21 日：http://www.spiceworks.com/voit/reports/windows-xp-end-of-life/.

儘管 Windows XP 作業系統即將終止支援，但其使用率仍非常普遍。Microsoft 過去也曾有許多 Windows 版本已終止支援，但沒有一個版本至今仍在普遍使用。Windows XP 之所以雄霸至今，原因之一可能是 2008 年的經濟危機造成許多企業資金短絀、裁員和撙節成本。[3] 此外，Windows XP 和其後繼系統 Windows Vista 之間只有五年的間隔，也或許還不足以讓企業有升級的動機，導致桌上型電腦汰換週期遲緩。

圖一顯示的資料讓人擔憂，因為仍有一大部分的桌上型電腦市場將暴露在與日俱增的威脅當中。當年 Windows XP 在 2001 年上市時，行動使用者的數量非常稀少，而且都是透過有線網路連線。當時，使用者大多經由企業掌握的網路上網，遠端存取則通常透過撥號連線。當年的 PC 威脅大多只會讓使用者困擾或是浪費時間，而非竊取重要資料。簡單言之，今日之所以要淘汰 Windows XP，正因為它是針對當年的時空背景設計的產品。

[3] Barbara Kiviat。(2013 年 9 月 16 日)。*Time*。「金融危機釋疑：為何我們還不曉得到底發生了什麼？」(Explaining the Financial Crisis: Why Do We Still Not Know What Happened?) 上次存取 時間 2014 年 3 月 21 日：http://business.time.com/2013/09/16/explaining-the-financial-crisis-why-do-we-still-not-know-what-happened/.

更換作業系統為何這麼難？

儘管迫在眉睫，但更換作業系統並沒有想像中的容易。IT 人員需預先料到升級會遇到哪些問題。根據 Dell 的一項研究顯示，作業系統移轉總是會帶來一些頭痛問題，[4] 例如應用程式相容性 (41%) 及使用者教育訓練和支援 (33%) 等等都是受訪者所指出的問題。此外，升級也可能會需要採購新的硬體，讓轉換過程不如想像順利。

Windows XP 會遭遇和 Java 6 相同的命運嗎？

2013 年 2 月，當 Oracle 宣布 Java™ 6 終止支援，不再提供安全更新來修補任何漏洞之後，駭客即開始強力鎖定該軟體未修補的版本。就在 Java 6 終止支援幾個月後，駭客便試圖攻擊 Java 的 CVE-2013-2463 漏洞，影響的範圍包括 Java 6 在內的多個版本。[5] 由於 Java 6 已不再獲得支援，Oracle 便不提供 (未來也不會提供) 安全更新給使用者。更糟的是，此漏洞攻擊已整合到 Neutrino 漏洞攻擊套件當中，未來將有更多同樣的攻擊得逞。

2014 年 4 月 8 日之後，Java 6 的情況同樣也將發生在 Windows XP 使用者身上，但 Windows XP 的威脅將遠勝於此。因為， Windows XP 和後繼 Windows 作業系統版本之間的共用程式碼，將成為駭客尋找待修補漏洞的「線索」。

總而言之，今日的威脅已和以往大不相同。事實上 Windows XP 的漏洞很可能讓整體企業及企業資料陷入危險當中。要防範這類已不再釋出修補程式的軟體漏洞，我們建議企業採用一套像趨勢科技 OfficeScan™ Intrusion Defense Firewall 入侵防禦防火牆這類的漏洞防護方案。漏洞防護技術的運作原理是，漏洞攻擊都會透過特定的網路途徑來攻擊應用程式。因此，我們可以藉由一些網路層的控管規則來管制進出目標軟體的通訊。

---

[4] Dell Inc.。(2013 年 9 月)。「淘汰 Windows XP：IT 人員調查」(Migrating Away from Windows XP: A Survey of IT Professionals)。上次存取時間 2014 年 3 月 21 日：https://www.kace.com/resource-center/resources/analyst-reports/Migrating_Away_from_Windows_XP_A_Survey_of_IT_Professionals.

[5] Gelo Abendan。(2013 年 8 月 27 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Java 6 零時差漏洞迫使使用者改用 Java 最新版本」(Java 6 Zero-Day Exploit Pushes Users to Shift to Latest Java Version)。上次存取時間 2014 年 3 月 21 日：http://blog.trendmicro.com/trendlabs-security-intelligence/java-6-zero-day-exploit-pushes-users-to-shift-to-latest-java-version.

企業會面臨什麼樣的潛在技術風險？

2013 年 10 月 Microsoft 公布一項消息表示 Windows XP 終止支援之後，該系統的感染情況將增加 66%，顯示駭客很可能會利用這段感染空窗期。[6] 駭客將試圖利用後續新版作業的安全更新來進行反向工程，藉此尋找 Windows XP 的漏洞。網路犯罪者甚至將「囤積」各種漏洞攻擊，待 Windows XP 支援終止時全面傾巢而出。[7]

一旦 Windows XP 支援終止，Internet Explorer® (IE) 也將成為另一個風險因素。該瀏覽器從 IE 8 之後的版本就不再支援舊版作業系統，這表示舊版作業系統的使用者將被打入冷宮。當然，使用者也可改用其他瀏覽器，不過，光更換瀏覽器仍不能 100% 防止瀏覽器漏洞。

另一項可能的技術風險是含有漏洞的端點裝置很可能被當成新一代惡意程式的攻擊跳板，因為舊系統很難對抗這些新的威脅。鎖定目標攻擊即經常利用軟體漏洞來入侵系統，讓企業暴露在資料竊盜和商業間諜的風險中，此外，任何使用 Windows XP 的 PC 對駭客來說都是一個明顯的弱點。

不更換作業系統會付出什麼代價？

老舊的系統和軟體若不淘汰，將帶來嚴重的企業風險，包括一些不可預期的潛在成本和後果。然而，也有人認為繼續使用 Windows XP 可以讓使用者不必再學一套新的作業系統，因為他們已經很熟悉系統的使用介面，而開發人員也對其瞭若指掌，這樣的主張看起來也很合理。

那麼，為何一定要更換系統？首先，IT 系統管理員應考量一下在終止支援之後繼續維護 Windows XP 的財務成本。決定繼續使用該系統的企業很可能必須加入客製化支援服務，也就是必須成為 Microsoft Premier Online 線上服務的會員。

但代價還不僅止於必須接受客製化支援服務。根據前述的 IDC 研究報告顯示，管理、支援及使用 Windows XP 系統遠較 Windows 7 系統來得昂貴。如表一所示，I T 花費在 Windows XP 營運作業的時間亦較 Windows 7 來的多。

---

[6] Gregg Keizer。(2013 年 10 月 30 日)。*Computerworld*。「Windows XP 感染率在支援終止之後可能暴增 66%」(Windows XP Infection Rate May Jump 66% After Patches End in April)。上次存取日期 2014 年 3 月 21 日：http://www.computerworld.com/s/article/9243660/Windows_XP_infection_rate_may_jump_66_aft er_patches_end_in_April.

[7] Dan Worth。(2014) 年 3 月 10 日)。*V3.co.uk*。「駭客囤積 Windows XP 漏洞攻擊準備在終止支援日當天一次爆發」(Hackers Hoarding Windows XP Exploits for Cut-Off Bonanza)。上次存取日期 2014 年 3 月 21 日：http://www.v3.co.uk/v3-uk/analysis/2333009/hackers-hoarding-windows-xp-exploits-for-cut-off-bonanza.

表一： IT 花費在營運作業上的平均時間	
Windows XP	Windows 7
營運作業	
3 小時	0.9 小時
停機時間	
2.9 小時	0.6 小時
使用者每年損失的時間	
9 小時	1.2 小時

資料來源：IDC 和 Microsoft

若無法立即更換系統會怎樣？

若企業仍必須繼續使用 Windows XP 系統，那麼我們建議企業採用一套白名單技術來維護一個較安全的企業環境。趨勢科技 Endpoint Application Control™ 端點應用程式控管解決方案可管制端點上執行的應用程式。這一層額外的防護可防止使用者在端點上安裝及執行任何不當、非經信賴或者惡意的應用程式，而且，也很容易隨趨勢科技 OfficeScan 這套端點防護方案一同部署和管理。

圖二： 為了支援多層式的安全防護，Endpoint Application Control 可以輕鬆與趨勢科技 Complete User Protection 使用者全方位防護解決方案整合，提供緊密連結的多層式威脅與資訊防護。

可以的話，升級作業系統是企業應立即採取的措施。然而，某些企業卻有不得已的苦衷，必須在 Windows XP 支援終止之後仍繼續維持該系統的運作。針對仍須繼續使用該作業系統的企業系統管理員，以下提供幾點最佳實務原則供您參考。儘管這些作法無法徹底解決現有問題，但若能確實遵行，將有助於企業避免一些將來的問題。

- **將 Windows XP 環境虛擬化。**如此可以多一層額外的防護，也讓管理更有效率。

- **在 Windows XP 區域網路上採用唯讀網域控制站 (RODC)，如 Windows 2008、2008 R2、2012 或 2012 R2。**為了有效管理，建議您在 Windows XP 系統連上的區域網路當中設置一台網域控制站，並將網域控制站設成唯讀模式。如此，您的系統管理員既能有效從遠端管理您的 Windows 電腦，又不會影響整體網路的安全。

- **在 Windows XP 電腦上套用最嚴格的安全群組原則。**儘管建議的設定應能符合您企業的需求，但仍強烈建議使用「專用有限安全功能」(SSLF) 群組原則設定。如需更多有關群組原則設定的最佳實務原則，請參閱 Microsoft 的「Windows XP 安全性指南」(Windows XP Security Guide) 以及「威脅與反制措施指南」(Threats and Countermeasures Guide)。[8]

- **可以的話，別讓 Windows XP 電腦與外界通訊。**必要時，手動更新第三方軟體。若無法避免跟外界通訊，可用網站代理器 (Web Proxy) 或應用程式防火牆來防護。

- **考慮採用其他瀏覽器。**企業或許免不了還是要使用 IE 瀏覽器，但可在其他任何瀏覽器都行不通時才使用 IE。

- **在區域網路上設置一台入侵防護 (IPS) 裝置。**您可以設置在交換埠分析器 (Switched Port Analyzer，簡稱 SPAN) 連接埠上，或者設在區域網路交換器與其他網路之間。

「在終止支援之後，企業內即使只有少數的 Windows XP 系統也會帶來嚴重的漏洞和安全風險，讓人很難認為它有保留的必要。有鑑於該系統無法徹底防範的威脅將越來越多，以及它對企業可能帶來的重大損害，強烈建議企業不應該再保留任何 Windows XP 作業系統。」

–Edward Ray，資深網路威脅研究員

[8] Microsoft。(2014 年)。*Microsoft Download Center*。「Windows XP 安全性指南」(Windows XP Security Guide)。上次存取時間 2014 年 3 月 21 日：http://www.microsoft.com/en-us/download/details.aspx?id=962; Microsoft。(2014 年)。*Microsoft Download Center*。「威脅與反制措施指南」(The Threats and Countermeasures Guide)。上次存取時間 2014 年 3 月 21 日：http://www.microsoft.com/en-us/download/details.aspx?id=24696.

此外，針對 Windows XP 使用者，趨勢科技特別延長了端點防護產品的支援，讓使用者在轉換至新版 Windows 作業系統時能減輕複雜度。已將企業端點裝置防護產品支援延長的趨勢科技 OfficeScan 和趨勢科技 Worry-Free Business Security™ 將可使用至 2017 年 1 月 30 日。[9] 而 OfficeScan 的 Intrusion Defense Firewall 入侵防禦防火牆外掛程式，還可在優異的用戶端防護之上添加一道網路層次的主機入侵防護 (Host Intrusion Prevention System，簡稱 HIPS) 來防範端點裝置上的漏洞，進一步強化端點防護。

在對抗鎖定目標攻擊方面，趨勢科技 Deep Discovery 可提供先進的威脅防護，即時發掘隱匿的威脅，此外，還提供了深入的威脅分析和可採取行動的情報來讓您評估、矯正及防範鎖定目標攻擊。

[9] 趨勢科技。(2014 年)。「趨勢科技針對 Windows XP 支援終止的正式聲明」(Trend Micro's Official Statement for Windows XP End of Support)。上次存取時間 2014 年 3 月 21 日：http://esupport.trendmicro.com/solution/en-us/1101907.aspx.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud