There is No Upside to Windows 7

RFG Perspective: Microsoft has notified its users that support for Windows 7 is ending, yet it is likely that many enterprises will not want to migrate off the software. RFG has performed a cost/benefits analysis and found that it is more economical to migrate or replace older hardware (and software) than to hold pat. Staying on Windows 7 and paying for extended operating system support on outdated hardware can be more than twice as expensive than the upgrade options. is the most expensive option. IT executives need to understand the options and their costs and act accordingly before the support window ends.

After 10 years of support, Microsoft will officially discontinue Windows 7 support on Jan. 14, 2020. Unfortunately, as of February 2019 the operating system remains extremely popular – 38 percent of all PCs and 44 percent of all Windows PCs run on Windows 7, according to NetApplications. For enterprises with large Windows 7 footprints, it may be impossible to migrate off all of them by the date of support discontinuance.

The somewhat good news is that Windows 7 users will have the option to pay Microsoft for software patches for another three years with what Microsoft calls "Windows 7 Extended Security Updates." But the support cost won't be cheap, and the price will increase each year. The availability of paid patches will finally terminate after three years in Jan. 2023. But the cost of extended support is the least of the extension worries for continued Windows 7 users.

Windows 7 Exposures

Microsoft states on its support page "While you could continue to use your PC running Windows 7, without continued software and security updates, it will be at greater risk for viruses and malware." Once flaws on Windows 7 are publicly known, there is a high probability that those exposures will be exploited for malicious purposes. After 2020, those enterprises that use Windows 7 that do not buy the extended support are at significant risk of attack even with firewall, antivirus, and anti-phishing protections in place. Risks and costs related to these known and unfettered attack vectors outweigh the costs of extended support and hardware/software upgrades. Executives that chose to pursue this path could be charged with malfeasance if the enterprise is hit with an attack that proves to be materially significant.

While security vulnerabilities are a major concern, there are other exposures enterprises need to be address. The first is that many of the new application updates that an organization uses may no longer run properly on Windows 7. This occurs because vendors follow Microsoft's lead (or their own philosophy of only supporting a limited number of operating system versions) and therefore no longer test their updates for patched or unpatched Windows 7 compatibility. Also, Microsoft is not committing to keep up with updating other functionality that may serve as necessary components of other Microsoft and third-party applications – updates apply to security patching only. The burden to address these shortcomings then becomes that of the enterprise, and in some cases, no acceptable or known solutions may exist outside of upgrading to Windows 10. It also means that going forward, there are multiple versions of these applications that must be catalogued, tracked, and supported if workarounds are required to maintain the base platform.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

The second problem is that new applications will require additional hardware and/or software features or capabilities over time. For example, newer applications may expect to have more memory available than is available or free on older PCs or require codecs or DLLs not released to Windows 7. Where a hardware solution is possible, IT will have to purchase add-on hardware to the old devices. Unsupported software may or may not work on Windows 7 and will require internal testing and patching processes that will prove increasingly challenging and, given exponentially expanding challenges, quickly outpace foregone upgrade costs.

The Cost/Benefit

Enterprises basically have three choices: stay with the old PCs and Windows 7; stay with the old PCs and upgrade to a Windows 10; or acquire new devices that will Windows 10. If a company chooses to stand pat, then it will have to pay for the Extended Security Updates, the added cost of incident problems, additional on-site support, and additional hardware expenses. The least expensive of these items is the cost for the Microsoft Extended Security Updates while potentially the biggest cost could be the loss of productivity by the users (normally not included in most analyses).

Upgrading old PCs to newer operating systems is not typically an advisable option. Most enterprises will wish to perform complete system wipes and software reinstalls from one or more golden images as the challenges of in-place upgrades make such an option ill-advised.. Plus, as with the first option, the now-ancient PCs are past their normal useful life and the numbers that will statistically suffer from increased breakages requiring telephone, remote desktop, and deskside support. The likely breakage increases will have a noticeable impact on support costs in the fourth year of PC service and a massive leap in the fifth year given mean-time-between-failures averages. These added incident problems, increased on-site support costs and additional hardware expenses, will quickly eclipse PC replacement costs – particularly when lost productivity is considered.

The replacement of old PCs running Windows 7 with new PCs and with a current operating system is the least cost option – whether purchased or leased. A recent RFG TCO analysis demonstrates that the least cost options for enterprise PC life cycles are repeating three-year or four-year leases over a five-year period. The most expensive option examined maintained old systems and handled break/fix issues as they arose irrespective on Windows 7 maintenance. Maintaining Windows 7 via extended support options added 60 percent or more costs to a current operating system base, further supporting three-year and four-year refresh strategies. RFG estimates that the minimum savings will be at least 12 percent for a lease over the purchase of new equipment. The savings between a new lease versus maintaining outmoded hardware could exceed 50 percent.

Summary

The half-life of IT equipment these days is less than three years. Firms that prefer to keep legacy hardware in production for five years or longer – beliefs frequently based in accounting principles – will find that amortization-based approaches to IT refreshes fail to account for rates of change, productivity improvements, and performance gains. The best option today is to not own PC

hardware but employ a three-year or four-year refresh policy to effectively minimize enterprise life cycle costs.

RFG POV: While Microsoft has provided users with an extended security support option for the next three years, enterprises should not see this as a justification to delay migrating off of Windows 7. While it may seem a preferable stop-gap to stave off PC and operating system upgrades, the financial and practical reality is that there is no upside to remaining on Windows 7 PCs any longer than necessary. IT executives should do their own benefits/cost analysis to determine their best course of action and then move forward as quickly as possible.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*