Industry White Paper

Windows 11 is a Security Initiative – A Key Rationale Overlooked by Organizations

Closed Loop Lifecycle Planning©
In collaboration with HP®, Microsoft®, and Intel®

January 2025

Submitted by: Jeff Malec, HP Principal Technologist, Lifecycle Planning
Bruce Michelson, Distinguished Technologist Emeritus HP and Close Loop LLC, Manager

About the Authors

Jeff Malec

Jeff Malec is an HP Principal Technologist and Lifecycle Planning Subject Matter Expert. After a 21+ year career with Microsoft, Jeff joined HP and is driving adoption of the modern workplace, Windows 11, and the related lifecycle elements.

Managing the Microsoft and HP relationship for several years, Jeff is an expert in go to market plans and customer adoption strategies.

Jeff holds multiple technical certifications from Microsoft.

Bruce Michelson

Bruce Michelson is an HP Distinguished Technologist (Emeritus) and the Manager of Close Loop LLC. Bruce has over 36+ years in delivering industry white paper and customer engagements. Bruce has delivered over 1,000+ white papers and over 350+ engagements.

Bruce is the author of seven books regarding aspects of lifecycle management. Bruce has numerous copyrights and patents regarding his expertise in User Segmentation, lifecycle management, cost of change, The Ready State©, and Appropriate Incumbent Behavior©.

Bruce teaches IT in Health Care and Advanced Systems and Design at Florida Atlantic University where he is an adjunct.

Bruce is sponsored by the HP, Microsoft, and Intel Alliance for this engagement.

Table of Contents

1.0 Management Summary

As of the writing of this White Paper, fewer than 12 months remain until Windows 10 reaches the end of its support period. On November 2, 2024, an article by TechSpot reported that Windows 11 adoption has now reached 35% and is continuing to rise, although Windows 10 still maintains a significant user base. This increase represents at least a 5% growth compared to previous periods. As more studies are conducted, it is anticipated that the migration to Windows 11 will accelerate.

Organizations are currently facing tight timelines not only for the tactical aspects of deploying a new operating system but also for understanding the broader implications of what the new operating system represents. In this White Paper, we will explore the key, and often overlooked, aspects of Windows 11. While some may perceive the messaging around Windows 11 as largely promotional, certain features, such as enhanced security, prepare the next generation of technology for future advancements.

Every organization is acutely aware of the volume and impact of cyberattacks, which have been relentless in 2024. Any reasonable security countermeasures should be considered for implementation.

Closed Loop Lifecycle Planning© states, "Change is inherently unsettling."

Windows 10 has been in use for quite some time, and there is a familiarity with the stability of the operating system. Deferring the adoption of a new version may be influenced by various factors, including emotional considerations. The reasoning is straightforward - if security improvements drive Windows 11, there would likely be an increased urgency to adopt the new operating system.

Developing business cases now typically involves identifying, defining, and quantifying benefits. In the post-pandemic era, IT initiatives often require detailed business cases due to competition for organizational budgets, with security frequently being prioritized and receiving funding first.

Priority-based budgeting is a concept discussed in the IT Strategies in the Post-Pandemic Era text, which emphasizes establishing priorities for IT organizations. Security consistently remains the top priority. When viewed through this lens, more organizations might have adopted Windows 11 well before the October 2025 end-of-support date for Windows 10.

1.2 Windows 11 Security Message

“Windows 11 is a security initiative, delivered by IT,” is a mantra developed with over 200 customer engagements around the Windows 11 transition.

According to Microsoft, Windows is “the most secure Windows operating systems to date.”

Security is top of mind for all organizations and across all industries. For the first time in memory, Windows 11 has a defined hardware baseline. That baseline is 8th generation of higher hardware, TPM 2.0, and secure core. All of these requirements are security driven to migrate to Windows 11.

Configuration management has always been a part of operating systems, but with a specific set of security requirements, Windows 11 is unique.

The overall Windows 11 messaging may have been overlooked by the perspective that Windows 11 is merely another traditional operating system upgrade. In this White Paper it is hoped that the security aspect of Windows 11 becomes highlighted more as a cybersecurity counter measure.

1.2 The "On-Ramp" Message

Windows 11 is often referred to as "the on-ramp to modern management." Closed Loop Lifecycle Planning describes modern management as "the cloud-first, highly automated, highly secure IT infrastructure based on end user requirements."

As organizations adopt modern management, the operating system must support the applications and provide the configuration and performance necessary for the Digital Employee Experience.

With elements such as Intune and Autopilot, completing the Windows 11 migration first can accelerate modern management projects.

Migration to modern management includes Windows 11 as part of the definition outlined above. As more organizations use Windows 11, security measures should be in place early so that IT infrastructure teams can focus on implementation within a secured operating environment.

2.0 Options Versus Defaults

Security features that were optional on Windows 10 are on by default on Windows 11.

By inquiring driven by Microsoft Copilot, the following response was provided which defines the optional versus default comparison.

According to Copilot:

*"Windows 11 comes with several **optional security features** that are enabled by default, many of which were also available in Windows 10 but are enhanced in the newer version. Here are some key features:*

1. ***Windows Defender Antivirus**: This built-in antivirus solution provides real-time protection against malware and other threats.*
2. ***Windows Hello**: A biometric authentication feature that allows users to log in using facial recognition or fingerprints, enhancing security without the need for passwords.*
3. ***BitLocker Drive Encryption**: This feature encrypts the entire drive, protecting data from unauthorized access, especially useful for devices that may be lost or stolen.*
4. ***Secure Boot**: Ensures that only trusted software is loaded during the boot process, helping to prevent malware from loading before the operating system.*
5. ***Virtualization-Based Security (VBS)**: Uses hardware virtualization to create a secure environment for sensitive operations, protecting against certain types of attacks.*

The emphasis on security is frequently overlooked as the primary motivation for the deployment of Windows 11. The list provided in this section offers insights into the validation of security-based requirements and their positioning within the default approach.

Cybersecurity remains a foremost concern across all industries, with ransomware continuing to be a prevalent threat that must be addressed. Endpoint devices are consistently targeted by cyberattacks, with phishing being a significant root cause of many successful breaches.

2.1 Windows 11 Is Likely Not the Last Default

Technology is advancing rapidly. Companies like HP, Microsoft, and Intel are integrating new security features to address emerging cyber-challenges. Ignoring these measures may indicate a lack of understanding or interest.

Modern hardware requires updated systems with TPM and secure core features. Future virtualization will enhance TPM, and the upcoming Pluton will set a new security standard.

As AI PCs and new operating systems are developed, security features will increase. IT and security teams should thoroughly examine the adoption of these advancements.

Organizations should consider device age, security improvements, and user needs when planning technology refresh cycles. This approach offers a more thoughtful perspective on upgrading technology.

3.0 Hardware Baseline

Microsoft setting hardware standards is unlikely to be the last instance of establishing baselines. Although plans are not publicly available or communicated, it is probable that establishing operating system baselines will become a prevalent consideration. The objective is to enhance endpoint security by implementing measures within the operating system that counter specific types of cyberattacks.

In future operating systems, the Pluton security processor may be considered for further baseline establishment. While Pluton was introduced in 2020 and is currently available, its integration represents a modernization of Trusted Platform Module (TPM) technology, potentially offering an additional layer of security.

As operating systems evolve and technology undergoes refresh cycles, there may be an increased focus on addressing device obsolescence through advanced security features.

4.0 Optimizations Overlooked

In all previous technology refresh cycles, readiness for the new operating system has always been a prerequisite. Similarly, Windows 11 requires organizations to prepare adequately for its implementation. However, Windows 11 readiness also involves anticipating modern management practices.

The adoption of a modern management solution is contingent upon ensuring that applications are ready to operate on Windows 11. This reliance is both technical and strategic in nature.

This section will provide examples of optimizations in Internet Explorer (IE), Application Programming Interfaces (APIs), and technical debt considerations. Windows 11 emphasizes the necessity of formally addressing these types of rationalizations to enhance organizational security.

As organizations plan their migration to Windows 11, compliance issues related to applications and hardware become critical factors that require immediate attention.

4.1 IE

IE has been retired since 2022. Most organizations have already addressed the retirement and are confident that the applications that required IE in Windows 10 have been remediated. While it is probable that the Windows 10 testing reflects Windows 11 compliance, it is not assured, so there should be similar testing to confirm that IE does not impact Windows 11 compliance.

4.2 APIs

APIs have become a newer target for the bad actors for cyberattacks. In many of the breach announcements required by regulations, it has been in some cases identifying third-party APIs as a root cause of security breaches.

Both internally created applications using third-party APIs should be rigorously evaluated.

4.3 Tech Debt

Tech Debt involves the costs and resources tied to outdated systems. Each industry has critical applications for specific tasks, which undergo significant updates over time.

The extent of documentation available is crucial for assessing an application's future readiness, including compatibility with Windows 11 and modern management practices.

To address Tech Debt alternatives are available including:

- Compatibility mode (available to 2029)
- Replace the application(s) which is often very costly
- Segment the application (placing the application on a specific non-integrated network so the overall IT infrastructure is secured)
- Containerization through virtualization alternatives
- LTSC which extends useful life but is specific in terms of updates and futures
- Adopting Extended Support, which while the costs are known may provide a timing to address reducing Tech Debt

The alternative could include doing nothing which is not really viable since the risk would outweigh benefits; however, it is a consideration.

From the security perspective, Windows 11 highlights Tech Debt and in many ways makes it impossible to ignore or address. Windows 11 in essence requires an organization to address the non-ready application portfolio.

4.4 Software In-Take

Software In-Take involves ensuring that both the existing portfolio of applications and new applications being considered and deployed are compatible with Windows 11. Compatibility is crucial for effective version control. Managing the number of supported versions of the same application often presents a software rationalization challenge.

Windows 11 emphasizes the importance of application compatibility and In-Take issues. Furthermore, addressing application vulnerability is a critical security matter that should not be postponed.

5.0 Governance

Governance includes policy, process, procedures, and workflows. In many ways, legacy governance defines how previous generations of products and services have been delivered and managed. Governance has not kept up with technology and often lags behind.

Windows 11 presents an opportunity to review and update governance practices. Many technologies, whether product or software, may necessitate changes to governance. If Windows 11 is considered a step towards modern management, the need for action is evident.

Governance typically involves cross-functional collaboration and includes all stakeholders. It often places additional responsibilities on organizations to follow new directions. Research by Closed Loop Lifecycle Planning on the Cost of Change© suggests that change is inherently unsettling. The transition enabled by Windows 11 is substantial.

Failing to adhere to governance can result in risks, including cybersecurity vulnerabilities. As delivery models evolve, such as on-premise, cloud, virtual, or hybrid, the related governance must also adapt.

Proactive governance should be established well before implementing new solutions, which is why governance often falls behind in organizations. Closed Loop Lifecycle Planning© also concludes that organizations have a limited capacity for change.

Governance may be as significant as the change itself. Adapting strategies requires new policies, processes, procedures, and workflows, which are challenging to implement. Governance acts as a security measure for change. If Windows 11 is seen as a catalyst for change, it necessitates the establishment of new governance rather than merely revising existing practices.

6.0 AI

Artificial Intelligence (AI), particularly generative AI, is a key initiative that every organization must consider. This necessity arises from the growing importance of consumer and demographic considerations, which demand attention and the integration of AI into business applications, including operating systems.

AI is not merely a trend; it is poised to become an integral part of IT infrastructure. As organizations develop AI governance frameworks, AI—exemplified by Microsoft Copilot—will be incorporated into every end user experience. The inclusion of AI elements in future versions of Windows operating systems enables quick scaling across an organization.

Windows 11, serving as the enabler for modern management, also facilitates AI integration. Although AI can operate on Windows 10, the security and performance enhancements are more pronounced with Windows 11, making it the preferred platform for AI deployment.

7.0 Tactical Versus Strategic - Conclusion

Historically, migrating to a new Microsoft operating system was perceived as a tactical move. While each upgrade brought new and appealing features, the transition process was like previous migrations. However, Windows 11, as a modern operating system, introduces distinct requirements and navigation elements that set it apart. The integration of modern management practices, default security features, and a defined hardware baseline collectively position Windows 11 as a strategic initiative rather than merely a tactical decision.

The distinction of Windows 11 as a strategic security initiative is important since Windows 11 is an integral part of the migration to new innovations.

Appendix

1. Closed Loop Lifecycle Planning - A Complete Guide to Managing Your PC Fleet, Bruce Michelson, published by Addison-Wesley Division of Pearson Education, ISBN 978-0-321-47714-9.
2. TechSpot, Windows 11 Reaches 35% Market Share, but Windows 10 Still Leads by Wide Margin, Skye Jacobs, November 2, 2024.
3. Microsoft website, as of March 12, 2022
4. Microsoft Security blog, as of March 12, 2022
5. Lansweeper, source for global Microsoft hardware baseline data as of April 2022, www.lansweeper.com
6. Lansweeper, source for global Microsoft hardware baseline data as of October 2022, www.lansweeper.com

Other Books by Bruce Michelson

1. Closed Loop Lifecycle Planning©, Client Computing in the Health Care Industry, by Bruce Michelson, Published by IDG, ISBN 978-1-61623-045-6.

2. Closed Loop Lifecycle Planning© - What It Is and Why It Is Important to You, by Bruce Michelson, Published by Bookmasters, ISBN 0-9667607-0-0.

3. We Are All Retail, The Race to Improve the Retail Experience in a Post Covid World, by Bruce Michelson and Leif Olson, Published by Archway Publishing, ISBN 978-1-6657-3394-6.

4. IT Strategies in the Post-Pandemic Era, Part of the Closed Loop Lifecycle Planning© Series, published by Archway Publishing, March 2023, ISBN 978-1-6647-3856-9.

5. Zero Trust, by Bruce Michelson and Cody Gerhardt, published by Archway Publishing, May 2023, ISBN 978-1-6657-4191-0.