WINDOWS 365

Cloud PC Deployment
Conceptual Architecture

Kevin Kaminski MVP
Kevin.Kaminski@bighatgroup.com
https://www.bighatgroup.com

Windows 365 Architecture
Document Changelog

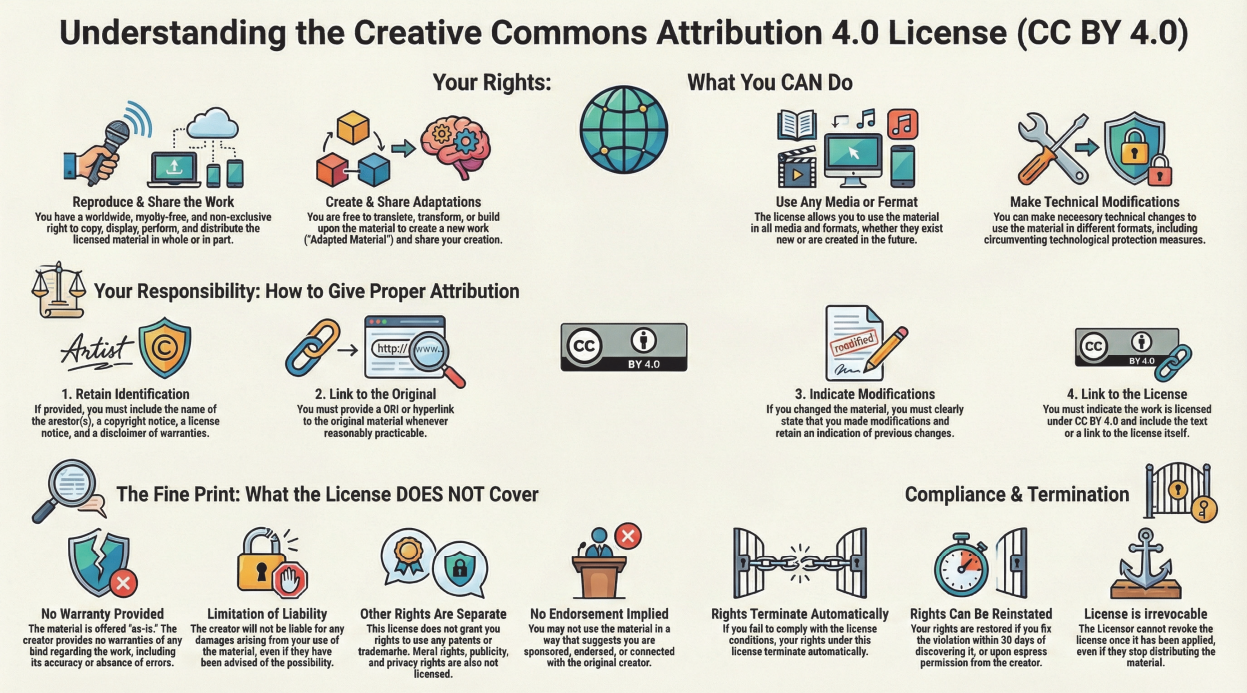
Version	Description	Author	Date
1.0	Complete Architecture	Kevin Kaminski	2026-1-8

Kevin Kaminski

Table of Contents

Table of Contents

1. License



2. About this Document

This document outlines the requirements and architecture of a Windows 365 Cloud PC reference design (originally developed by Kevin Kaminski as an educational tool). It presents high-level technical details for a Windows 365 pilot deployment, serving as a roadmap and decision guide to help technical teams identify the components needed to build the environment.

2.1. How to Use This Document

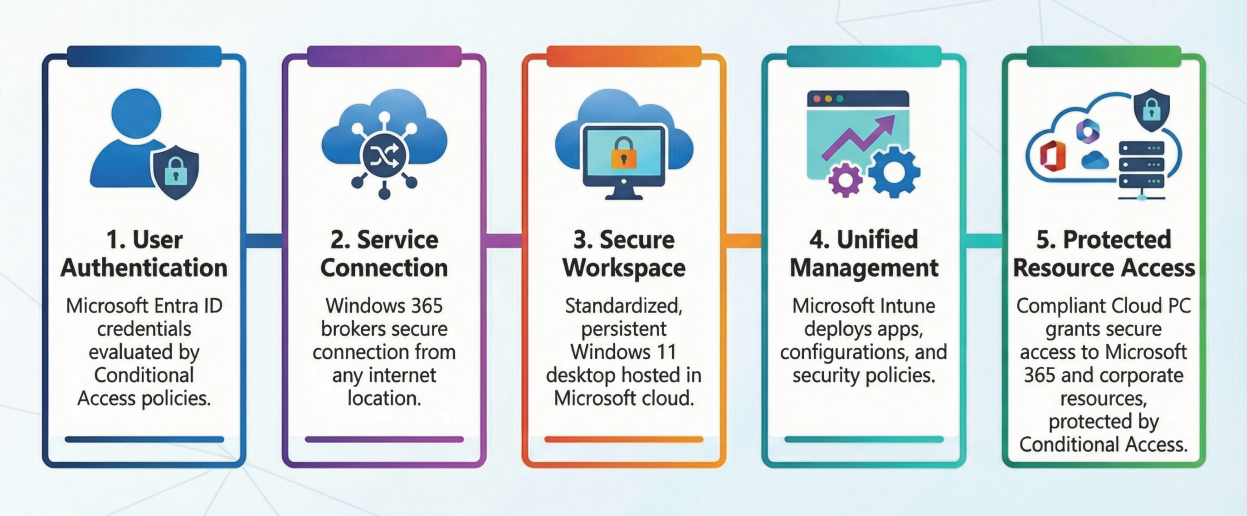
IT professionals and architects should use this document to understand the design principles and components of a Windows 365 pilot deployment. It serves as a foundation that can be extended to support more complex Windows 365 Cloud PC solutions as needed.

2.2. Audience

This reference is intended for technical specialists and IT staff and guides configuration and support throughout the Windows 365 Cloud PC deployment. Additionally, managers and directors should familiarise themselves with the design and governance framework in preparation for the operational shifts and new management workflows introduced by the Cloud PC environment.

3. Overview

This Windows 365 reference design (authored by Microsoft MVP Kevin Kaminski) helps organisations envision the architecture required for a successful Cloud PC deployment. It outlines a standard implementation strategy to deliver a reliable, flexible, and cloud-native computing experience.



Following a comprehensive assessment of the environment, this document presents technical recommendations to align with a typical implementation's core objectives:

- **Ubiquitous Access:** Seamlessly enabling a "work from anywhere" user base through persistent cloud-based desktops.
- **Modern Security:** Providing a secure, isolated, and compliant compute environment integrated with Microsoft Entra ID.
- **Simplified Management:** Streamlining the lifecycle of corporate endpoints via the Microsoft Intune admin centre.

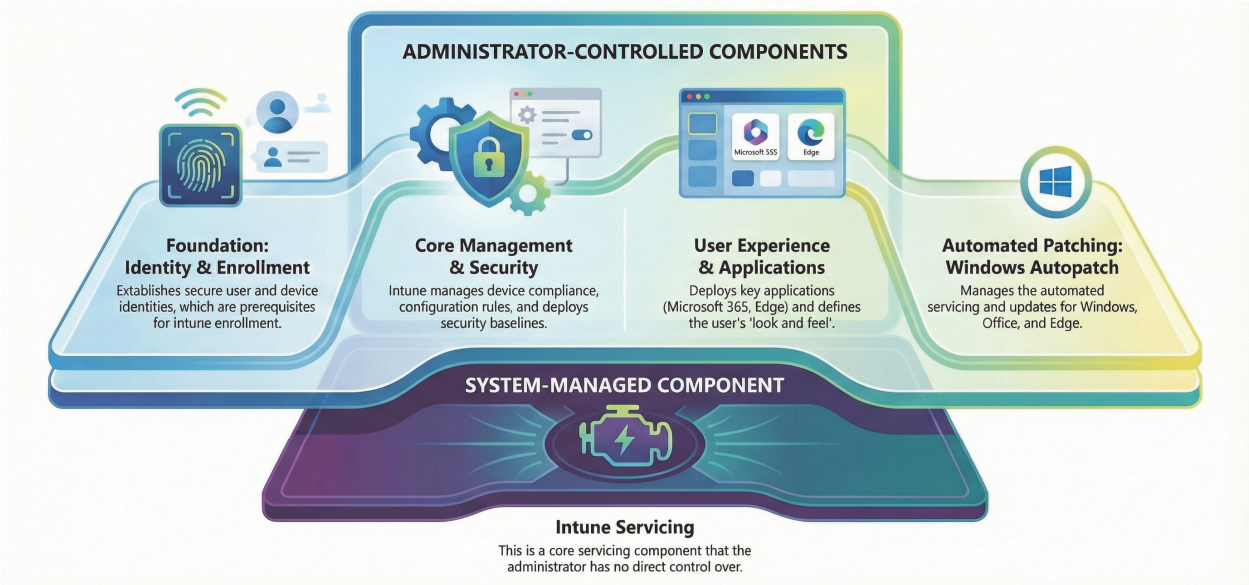
Key Design Recommendations

To ensure a scalable and efficient deployment, the following architecture is proposed:

- **Cloud-Native Identity:** Cloud-Native Identity, all Cloud PCs will be joined directly to Microsoft Entra ID (Azure AD), eliminating any on-premises identity dependencies.
- **Automated Provisioning:** Deployment will utilise Windows 365 Provisioning Policies to automate the delivery of Cloud PCs based on user group membership.
- **Unified Management:** All Cloud PCs will be automatically enrolled in Microsoft Intune for configuration, application delivery, and security policy enforcement.
- **Optimised Connectivity:** The design prioritises the use of the Microsoft-hosted network to simplify the initial deployment footprint.
- **Project Scope and Impact**

This pilot is more than a simple virtual desktop proof of concept; it represents a fundamental shift toward a modern workspace model. By leveraging cloud-native technologies, the organisation will move away from hardware-bound management to a more ubiquitous, cloud-based solution. This approach yields greater organisational value, improved disaster recovery readiness, and a better user experience.

The following points represent the core architectural pillars of the Windows 365 solution as outlined by the design:



Identity

- **User Identity:** By leveraging cloud-native technologies, the organisation can transition away from traditional hardware-bound management toward a ubiquitous solution that delivers greater organisational value, improved disaster recovery, and a better user experience.
- **Device Identity:** Cloud PCs are joined directly to Microsoft Entra ID (Entra Join), establishing them as trusted corporate assets and removing dependencies on legacy on-premises domain controllers.
- **Enrollment:** Cloud PCs enrol automatically into Microsoft Intune during provisioning for management and security enforcement.

Cloud Management

- **Intune:** Intune serves as the primary management platform (a single pane of glass) for the entire Cloud PC lifecycle, including configuration and software delivery.
- **Device Compliance:** Defines health requirements (firewall active, real-time AV protection, etc.) that a Cloud PC must meet to access corporate data.
- **Device Configuration:** Uses cloud policies (Settings Catalogue) to enforce granular security settings over the internet, ensuring the Cloud PC is secure regardless of user location.

- **Modern Application Management:** Replaces traditional OS imaging with cloud-native software deployment methods such as the Intune Management Extension. This approach ensures apps are delivered and updated without building and capturing monolithic images.
- **Intune Security Baselines:** Implements pre-configured, industry-standard Microsoft security settings to harden the operating system and core applications quickly.

User Experience

- **Look and Feel:** The default look and feel that comes with the Windows 365 Cloud PC image will be used. A configuration profile will unpin the Store from the taskbar as the user doesn't need it.
- **Start Menu and Taskbar:** A curated "Day One" interface that pins essential tools to reduce cognitive load, while still allowing users to personalise their workspace afterwards.

Applications

- **7-Zip:** Provided as a standard utility for file compression and decompression tasks required for document management.
- **Edge:** The primary enterprise browser, configured with single sign-on (SSO) and security policies to protect the main gateway to web-based resources.
- **Microsoft 365:** The core productivity suite (Word, Excel, Outlook, and Teams), included in the base image and kept current via the Monthly Enterprise Channel.
- **VLC (UWP):** A lightweight media player available as an optional install for users who need to view training videos or corporate communications.
- **Company Portal:** A self-service application store that allows users to install approved software on demand without needing local administrative rights. This is the user's portal for all their Intune activity and can help with more than just their Cloud PC if they have more devices managed by Intune.

Servicing

- **Windows Autopatch:** An automated service that manages update orchestration and monitors device health, significantly reducing the manual burden on IT staff.
- **Windows Servicing:** The "Windows as a Service" model that ensures the OS receives a continuous flow of security and feature updates.
- **Microsoft 365 Apps Servicing:** Extends automated patching to the Microsoft 365 stack to ensure productivity tools are always hardened against evolving threats.
- **Edge Servicing:** Automates browser updates across the fleet using a progressive rollout model to detect and mitigate potential web-app compatibility issues early.
- **Intune Servicing:** Reflects the evergreen nature of the management platform itself, which receives monthly updates with new capabilities and enhancements.

3.1. Design Overview

3.2. Solution Strategy

Big Hat Group Inc. recommends and utilises phased deployment strategies in accordance with industry best practices. This approach ensures that each phase addresses the specific requirements, challenges, and opportunities unique to the different layers of an enterprise-level, end-user computing strategy.

By leveraging modern cloud services to break dependencies on legacy IT systems, these solutions are engineered to realise the lowest TCO (Total Cost of Ownership) and maximise long-term business value. The solution design strategy will adopt the following high-level principles:

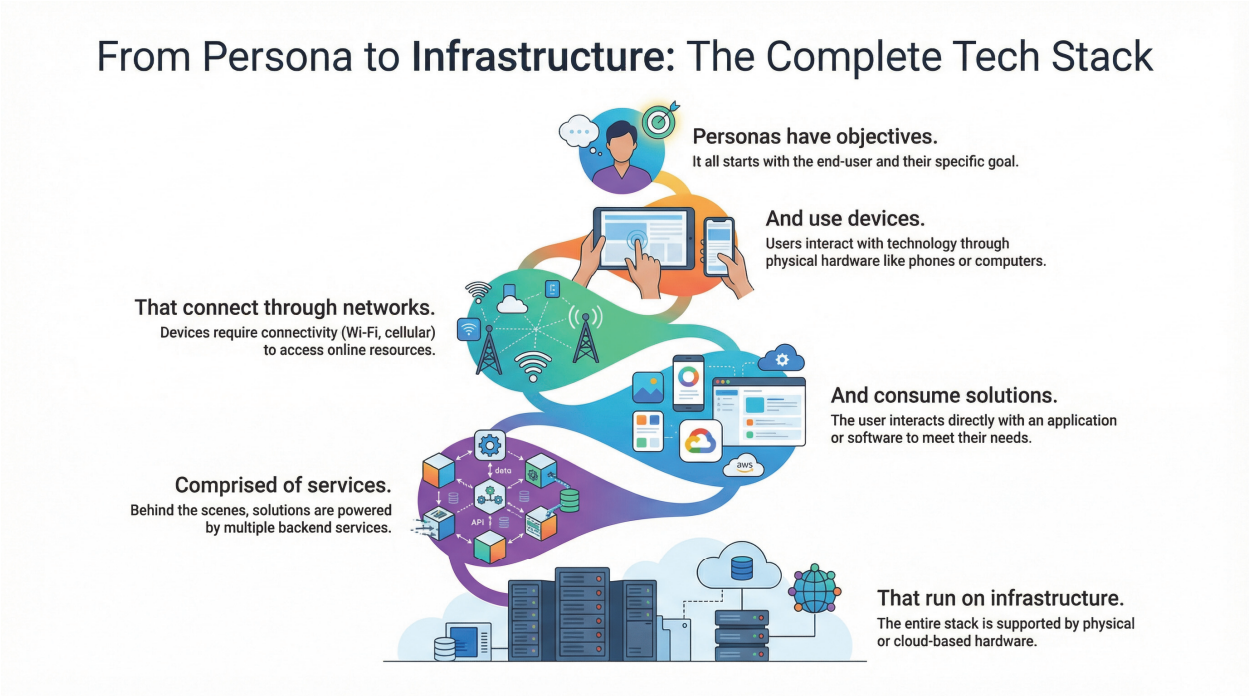
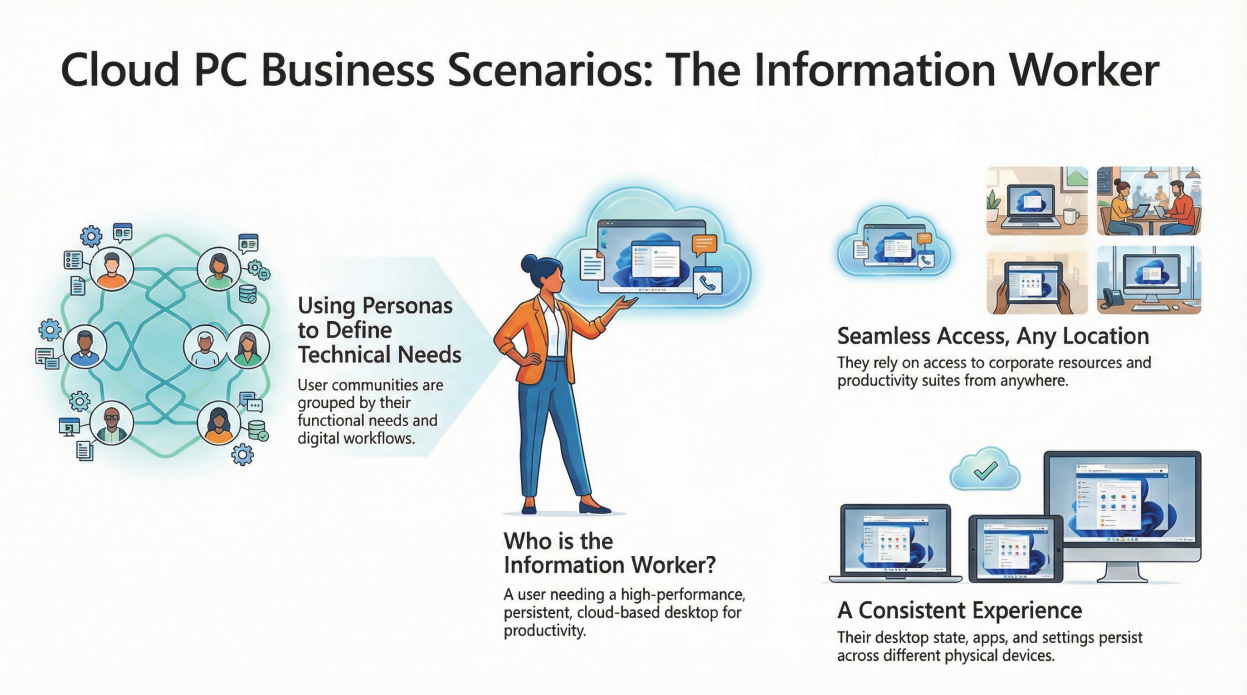


Figure 1. Design Process.

By categorising users into personas, we can identify the specific daily objectives that drive their technology needs. During a digital transformation, we must ensure that individual updates, such as a Cloud PC, align with the broader organisational strategy. While modernisation aims to replace legacy systems, some personas may require "bridging solutions" to transition smoothly without disrupting their work. Some may use Cloud PCs to enhance their work rather than replace their company-issued laptop or desktop.

This guide presents an information worker scenario using Windows 365 from an unmanaged device, such as a user's personal device at home. The core of this solution will be the Intune configuration, which serves as the management plane. These chapters help explain scenarios, decisions and an overall vision for your Windows 365 environment. The infographic below examines the design from an Intune and Entra perspective, where most of the work is required. Reflect on these key design components and recommendations as we explore the conceptual design process for Windows 365.

For this initiative, the following user persona has been identified: Cloud PC Information Worker



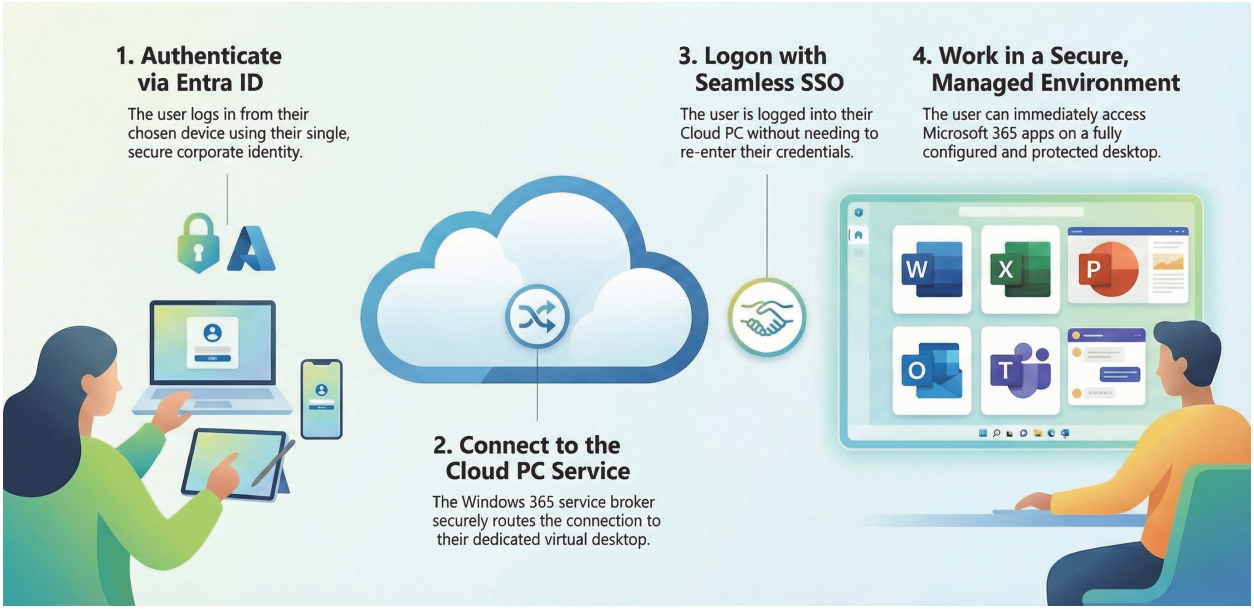
3.2.1. User Persona

Each user persona has specific technical objectives. For the Windows 365 Information Worker persona, those objectives include:

- Secure access from any device
- A secure managed Cloud PC workspace.
- Access to Microsoft 365 and web-based applications
- Data backup

Persona: Windows 365 Information Worker
The Information Worker persona represents users who require a high-performance, persistent cloud-based desktop. This persona is designed for staff who rely on seamless access to productivity suites and corporate resources from any location, utilising Cloud PC technology to maintain a consistent state across various physical endpoints.

The architecture can be boiled down to the following for an information worker at a conceptual level. They use a random range of devices to connect to their Cloud PC using Entra ID. Once connected, the user has access to a trusted and secure workspace to perform their work.



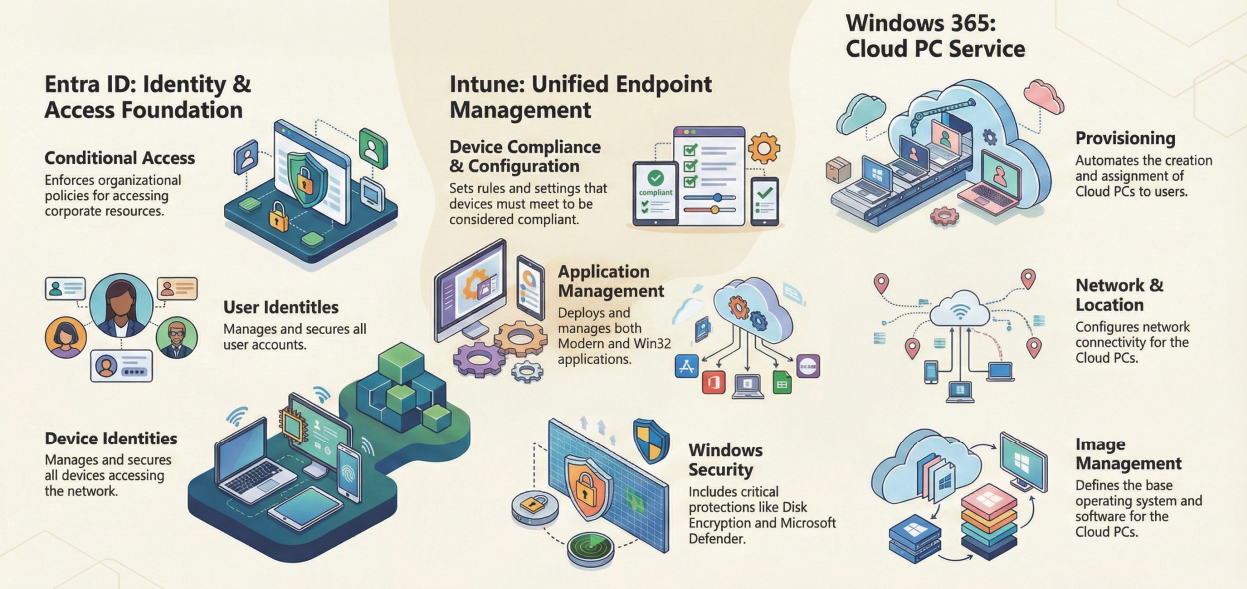
Key Technical Attributes:

Persistence: Users are assigned a dedicated Cloud PC instance, ensuring that application state, browser tabs, and personal settings persist between sessions.

- **Standardised Management:** The environment is fully managed via Microsoft Intune, receiving automated updates, security policies, and application deployments.
- **Identity Integration:** Leveraging Entra ID for both user and device identity, enabling a Single Sign-On (SSO) experience and robust Zero Trust security through Conditional Access.
- **Productivity Baseline:** A pre-configured application stack including Microsoft 365 Apps, Edge, and essential utilities, ensuring the user is productive immediately upon first login.

3.2.1.1. Persona Technical Requirements

These requirements define the standard configuration for the Information Worker persona. This persona is designed to provide a high-performance, secure, and standardised productivity environment delivered via the Windows 365 Enterprise service.



3.2.1.2. Cloud PC Information Worker Persona

The Information Worker persona is optimised for users who rely on the Microsoft 365 productivity suite and web-based line-of-business applications.

- **Cloud PC (Enterprise):** Leveraging the Enterprise edition allows for full integration with Microsoft Intune, providing granular control over the device lifecycle.

  This ensures that Cloud PCs are provisioned within the organisation's Entra ID tenant with Intune management, enabling direct connectivity to internal resources and simplifying license management via the Microsoft 365 Admin Centre.

3.2.1.3. Identity & Access Management

The solution utilises a "Cloud-First" identity model to simplify the user experience and strengthen security.

- **Entra ID User Identity:** Users will authenticate using their primary corporate credentials. This enables Single Sign-On (SSO), meaning that once the user logs in to the Windows App, they are automatically authenticated to Microsoft 365 apps, Edge, and other integrated services.

- **Entra ID Device Identity:** Each Cloud PC will be Entra Joined. This allows the device itself to be recognised as a trusted corporate asset.

  This identity serves as the primary signal for Conditional Access policies to verify that the device is managed and compliant before granting access to sensitive data.

3.2.1.4. Application Stack

The following applications comprise the base image for this persona, ensuring users are productive from the first login.

Core Applications: (In Image)

- **Microsoft 365 Apps:** The core productivity suite (Word, Excel, PowerPoint, Outlook, and Teams). These will be deployed via the Windows 365 image gallery, ensuring they remain up to date via the Monthly Enterprise Channel for stability.
- **Microsoft Edge:** Configured as the primary browser with sync enabled. Policies will be applied to manage security settings, extensions, and enterprise site lists for legacy compatibility.

Utility & Media Tools: (Required)

- **7-Zip:** Deployed as a required Win32 app to handle various compression formats as are necessary for document management and file compression.
- **Remote Help:** Available with recently revised licensing, this enables IT to support users who are in a zero-trust environment but still need the assistance of IT.
- **Company Portal:** This acts as the self-service store. It allows Information Workers to install optional, approved applications on demand without requiring local administrative rights, reducing help desk tickets.

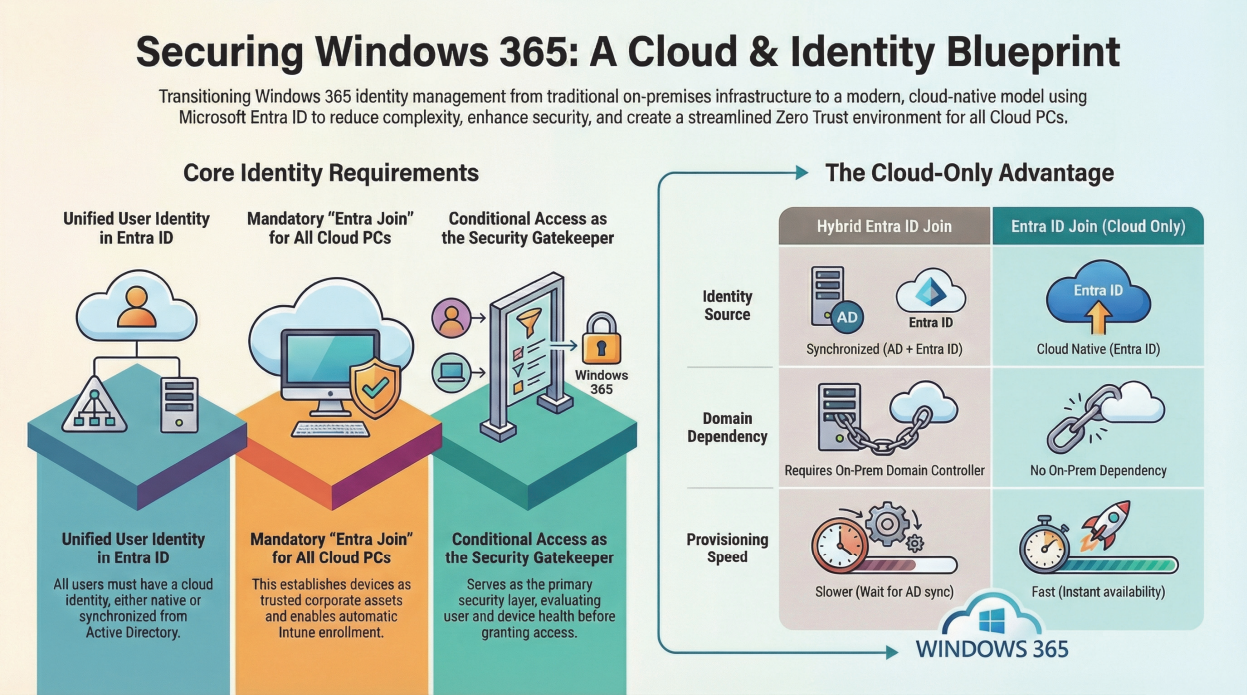
Utility & Media Tools: (Available)

- **VLC Player (UWP):** Provided via the Microsoft Store (Universal Windows Platform) to offer a lightweight, secure, and versatile media player for training videos and corporate communications.

3.2.2. Cloud and Identity

The Windows 365 solution requires full integration with the identity services hosted within the Microsoft Entra ID tenant. While existing on-premises infrastructure, such as Active Directory, can influence administrative roles, the primary design goal is to use a cloud-native model to reduce technical debt and complexity. In an ideal architectural state, legacy identity dependencies are removed, allowing all users and devices to be managed directly within Entra ID and secured by Zero Trust-based Conditional Access policies.

This shift fundamentally redefines identity management. Active Directory was once the primary identity authority, but the rise of cloud-native applications now demands a fully cloud-native identity approach (via Microsoft Entra ID).



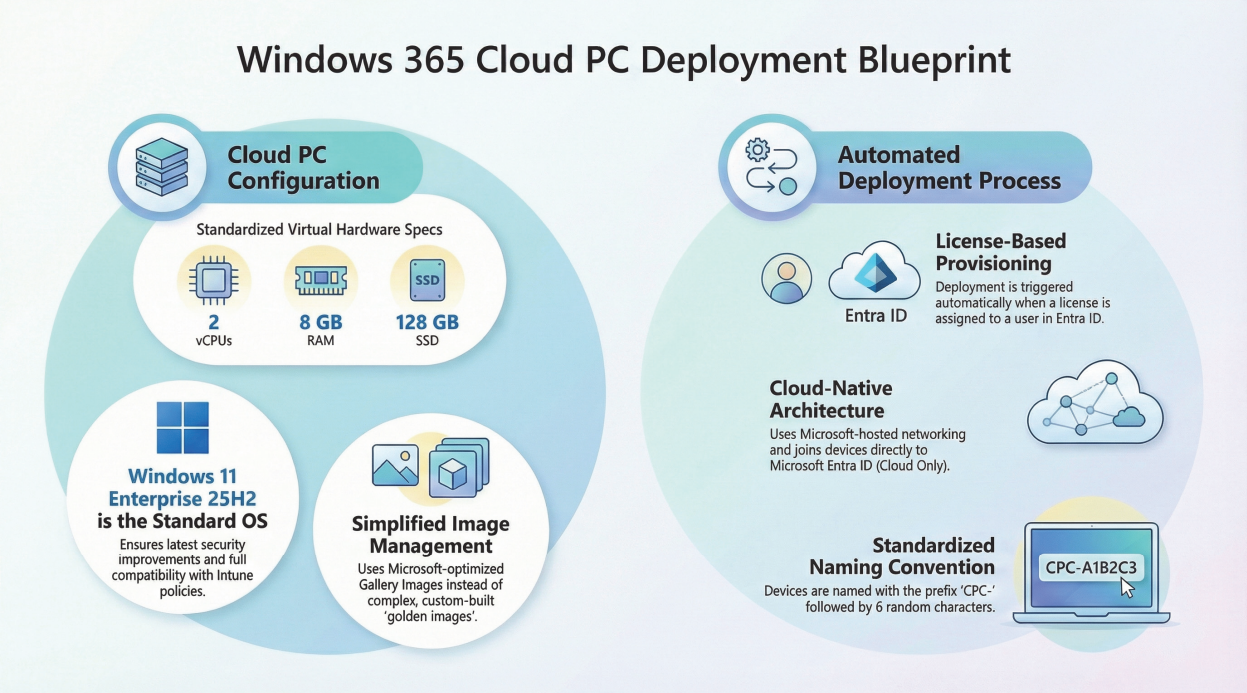
Identity Requirements and Integration

To ensure successful deployment, the following identity standards will be enforced:

- **User Identities:** At a minimum, all users of the solution must have an identity present in Entra ID to be eligible for a Cloud PC assignment. These identities can either be created natively in the cloud or synchronised from an on-premises Active Directory environment using Entra Connect. Users of this solution will use accounts with their source set to Entra ID.
- **Administrator Identities:** Much like user identities, the best practice is to have your administrators for Intune as cloud identities. Different conditional access policies may be used to further validate these logins, such as requiring phishing-resistant MFA.
- **Device Identities:** All Cloud PCs will be joined directly to Microsoft Entra ID. This "Entra Join" state is a mandatory prerequisite that enables automatic enrollment into Microsoft Intune for comprehensive Mobile Device Management (MDM). This allows devices to provision quickly when they connect to Entra ID.
- **Access Security:** Once the identity is established, Conditional Access will serve as the primary security layer, evaluating the user's identity before granting access to the virtual desktop environment and re-evaluating the logon from the Cloud PC to Microsoft 365, with the Cloud PC's compliance being evaluated. This is to ensure that BYOD devices can still log onto the Cloud PC from an unmanaged device.
- **Groups:** To support the design, there will be a group needed for Cloud PC user accounts and another for Cloud PC devices. A third group is required for Cloud PC administrators. These groups will be based on Entra ID to as they cannot be based in Active Directory.

3.2.3. Provisioning

The Windows 365 architecture is built upon the principle of decoupling the operating system from physical hardware, transforming the traditional PC into a scalable, cloud-delivered service. This strategy ensures that the "Information Worker" persona receives a high-performance, persistent environment regardless of the physical endpoint used to access it.



Virtual Hardware Specifications

For the pilot deployment, the Cloud PC resources are standardised to meet the performance requirements of an information worker's productivity requirements:

- **Compute Power:** Each Cloud PC is provided with two vCPUs to ensure responsive application performance.
- **Memory:** 8 GB of RAM is allocated to support multitasking across Microsoft 365 apps and web-based line-of-business tools.
- **Storage:** A 128 GB Standard SSD provides ample space for the OS, applications, and local cache, while primary data storage is directed to the cloud. This disk size is the minimum required for a custom image if you want to replace it later.
- **Operating System Standard (Windows 11 Enterprise 25H2)**

The solution utilises a "Dynamic Cloud PC" philosophy, mandating the use of the latest stable version of the operating system to eliminate technical debt:

- **Baseline Version:** Windows 11 Enterprise 25H2 serves as the standard image.
- **Image Management:** To reduce complexity, the design utilises Microsoft-optimised Gallery Images from the marketplace rather than thick, custom-built "golden images".
- **Optimisation:** The 25H2 standard ensures full compatibility with the latest Intune administrative templates and provides kernel-level security improvements.
- **Automated Deployment and Provisioning:**

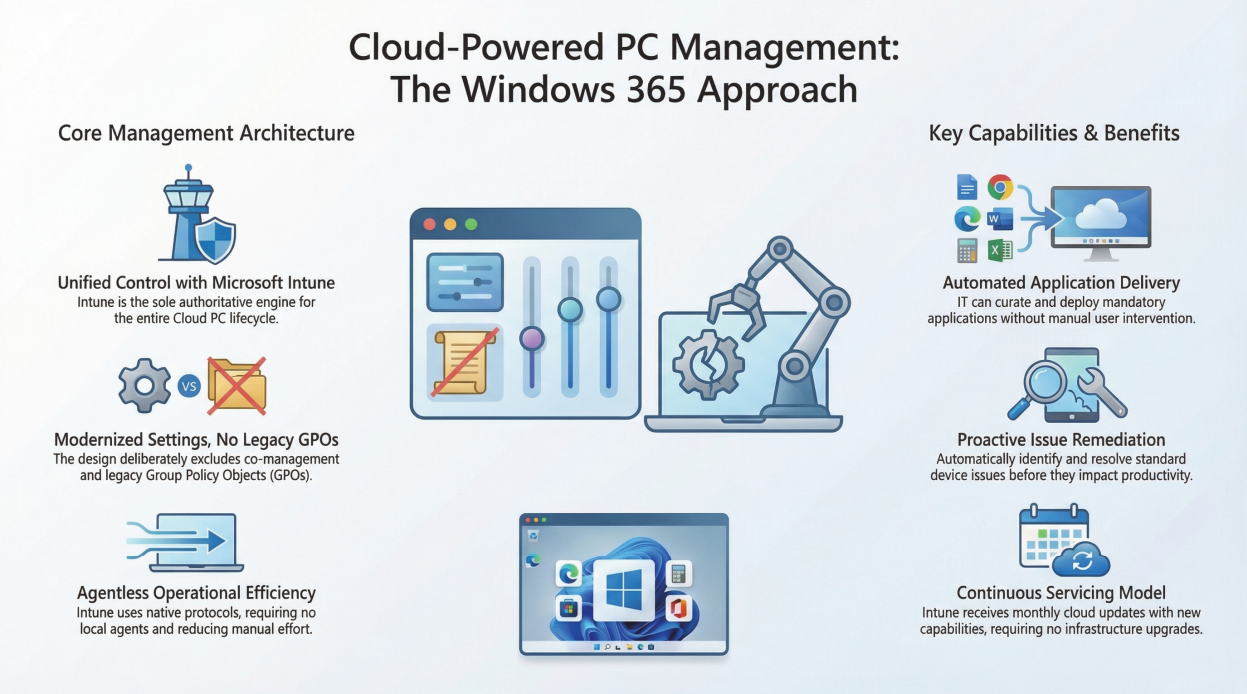
  The deployment process is fully automated via Intune, replacing legacy imaging tools such as the Microsoft Deployment Toolkit. With this method, images are still used to provision the Cloud PC, but the result depends on the overall design. Below are key provisioning details for the deployment:

  - **Provisioning Policies:** Deployment is triggered automatically by assigning a Windows 365 license to a user within a targeted Entra ID group.

- **Network Connectivity:** The solution utilises the Microsoft-hosted network for initial deployment to simplify the infrastructure footprint and ensure high-speed cloud access.
- **Cloud-Native Join:** All devices are joined directly to Microsoft Entra ID (Cloud Only), removing dependencies on on-premises Domain Controllers and reducing provisioning latency.
- **Device Naming:** Must use a randomised name, yet use a prefix to be easily identified.

3.2.4. Management

The management architecture for the Windows 365 environment transitions from legacy, infrastructure-heavy systems to a modern, cloud-native architecture. This design prioritises a "cloud-only" management strategy to ensure administrative agility and reduced operational overhead.



Microsoft Intune: The Management Authority

- **Unified Control:** Microsoft Intune serves as the sole authoritative engine for overseeing the entire lifecycle of the Cloud PC.
- **Policy Enforcement:** The solution utilises Configuration Service Providers (CSPs) and the Settings Catalogue to enforce policies over the internet, ensuring devices remain secure regardless of the user's physical location.
- **Remote Help:** The solution for assisting users who are in a zero-trust configuration. Older methods allowed for direct connections to machines, but Remote Help is the new cloud-based method of assisting users.
- **Modernisation of Settings:** By establishing Intune as the single management authority, the design deliberately excludes co-management and legacy Group Policy Objects (GPOs) to maintain a streamlined administrative experience.

Agentless Operational Efficiency

- **Reduced Overhead:** Intune handles configuration settings using native Mobile Device Management (MDM) protocols, requiring no local agents.

**There is a dependency on the Intune Sidecar to download and run installers and scripts.*

- **Automated Maintenance:** System administrators can automate configuration updates and maintenance tasks, significantly reduce manual effort and improve consistency across the fleet.

Application Lifecycle and Distribution

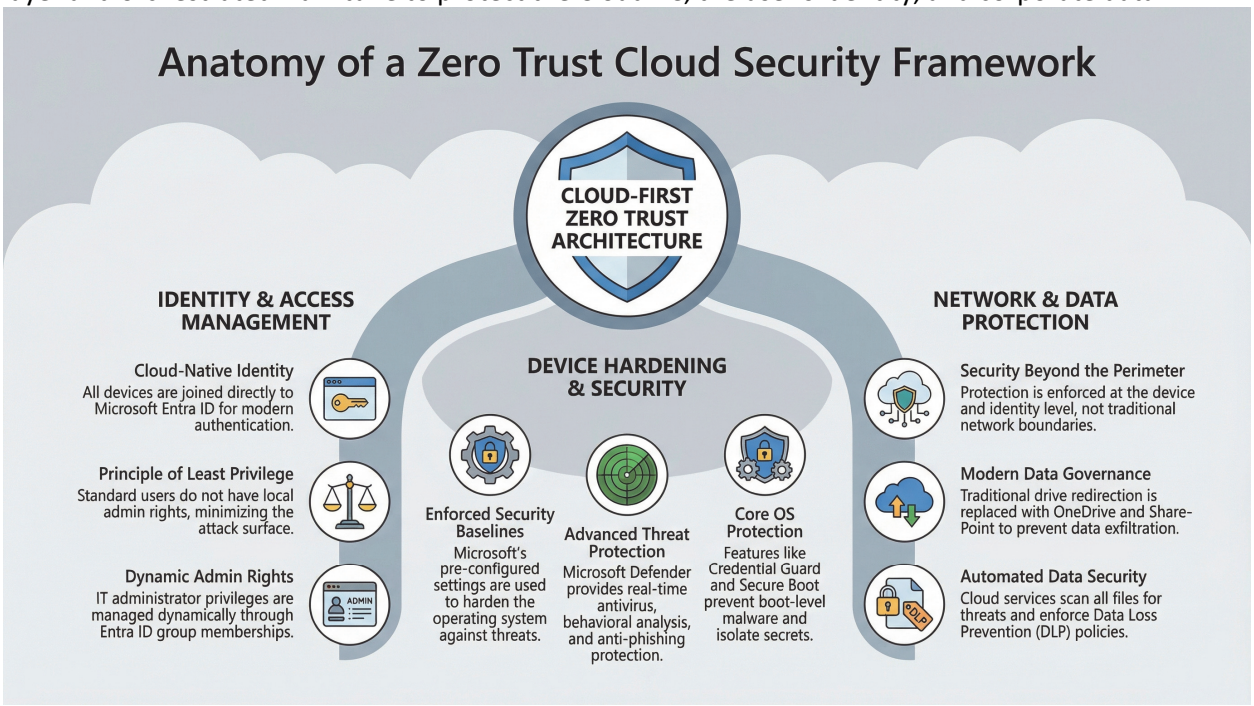
- **Automated Delivery:** IT administrators utilise Intune to curate and deploy mandatory applications, ensuring users have access to required tools without manual intervention.
- **Proactive Remediations:** The management framework includes the execution of proactive remediations to identify and resolve standard device issues before they impact user productivity.

Continuous Servicing Model

- **Management as a Service:** Because Intune is a cloud-native service, it receives monthly updates that introduce new capabilities and security enhancements without requiring manual infrastructure upgrades.
- **Operational Rhythm:** The IT team will adopt a proactive rhythm for monitoring service changes via the Microsoft 365 Message Centre to ensure the architecture remains aligned with the latest management best practices.

3.2.5. Security and Access

The security and identity framework for this engagement is built on a "Cloud-First" architecture designed to establish a resilient Zero Trust environment. Security is baked into the operating system layer and orchestrated via Intune to protect the Cloud PC, the user's identity, and corporate data.



3.2.5.1. Identity and Access Management

Entra ID Join: All Cloud PCs are natively joined to Microsoft Entra ID (formerly Azure Active Directory), establishing a cloud-first identity foundation. This eliminates the dependency on traditional on-premises domain controllers, enabling seamless provisioning, management, and authentication over the internet. Entra ID Join enables Cloud PCs to participate fully in modern identity-driven services, including Conditional Access, passwordless authentication, and seamless Single Sign-On (SSO) with Microsoft 365 and other cloud-based applications.

Least Privilege: By default, Cloud PC users are provisioned without local administrator rights. This aligns with the principle of least privilege and significantly reduces the potential attack surface by limiting the ability to install unauthorised software or alter system configurations. All application deployment and device configuration is centrally managed through Microsoft Intune, ensuring that only approved tools and settings are applied, and that system integrity is preserved across the Cloud PC fleet.

Admin Access: Administrative privileges for IT personnel are managed through Microsoft Entra ID group memberships. These groups are linked to an Intune configuration profile for configuring the local administrator group on the device. This eliminates the need for persistent admin accounts on endpoints, providing a secure, auditable, and role-based elevation model that supports modern Zero Trust operations. Access can be revoked via group membership.

- **Entra ID Join:** All devices are joined directly to Microsoft Entra ID.
- **Least Privilege:** Standard users are not granted local administrator rights to minimise the attack surface.
- **Admin Access:** IT administrator rights are managed dynamically through Entra ID Group memberships and deployed via an Intune configuration profile.

3.2.5.2. Device Hardening and Security Baselines

To ensure every Cloud PC maintains a secure and trusted execution environment, the solution enforces Microsoft's recommended Security Baselines. These baselines are delivered through Microsoft Intune and enable a consistent set of hardened configurations across all Windows 365 devices, reducing risk and simplifying compliance with security best practices.

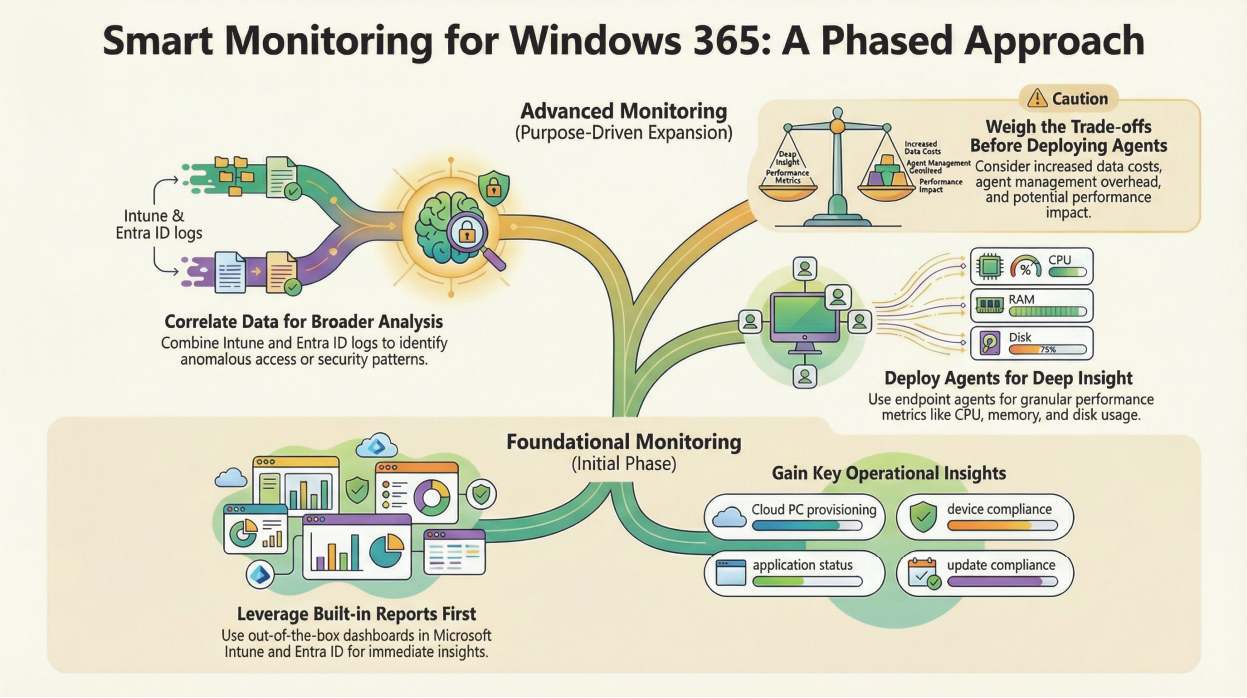
- **Operating System Hardening:** Core Windows 11 security technologies are enabled by default, including Credential Guard, which uses virtualisation-based security (VBS) to protect authentication secrets from credential theft attacks, and Secure Boot, which ensures that only trusted, signed boot components are loaded during system startup. These features create a secure foundation for the Cloud PC.
- **Advanced Threat Protection:** Microsoft Defender Antivirus is configured to provide always-on, real-time protection with cloud-delivered threat intelligence and automated remediation. Microsoft Defender SmartScreen adds an additional layer by blocking access to known malicious websites

and preventing the execution of suspicious or unverified applications, enhancing protection against phishing and malware.

- **Host-Based Firewall and Traffic Control:** Windows Defender Firewall is enforced through Intune policies to apply granular inbound and outbound traffic filtering. This isolates each Cloud PC from unnecessary lateral communication and enforces strict segmentation between devices, supporting Zero Trust network principles even within the cloud-hosted environment.
- **Data Protection and Disk Encryption:** Although the underlying infrastructure benefits from Azure Disk Encryption, typically, Intune is used to apply encryption configuration and compliance policies at the OS level. However, since this is a hardware-level service, configuration and monitoring are not required. This ensures that all Cloud PCs meet organisational data protection standards and that the virtual storage layer remains secure against unauthorised access, even when abstracted from the physical hardware.

3.2.6. Monitoring

Effective monitoring is a foundational requirement for operating a Windows 365 environment at scale. The solution must collect sufficient telemetry to enable proactive management, operational troubleshooting, and security investigation, while balancing cost, complexity, and administrative overhead.



3.2.6.1. Built-in Reports

Windows 365 provides several built-in reports and dashboards across Microsoft Intune and Entra ID, offering immediate value with minimal configuration. These out-of-the-box insights support common operational scenarios, including device health checks, application deployment status, update compliance, and user sign-in activity. For day-to-

day operations and rapid triage, these native reports are sufficient and are the first layer of monitoring.

3.2.6.2. Azure Monitor

For more advanced scenarios, monitoring data is correlated across platforms. Combining Intune device telemetry with Entra ID sign-in and Intune platform logs enables broader analysis, such as identifying anomalous access patterns, sign-ins from non-compliant or unfamiliar devices, or user experience issues tied to conditional access enforcement. This cross-service visibility becomes increasingly important as the environment scales and as security requirements mature.

Once Azure Monitor is configured, additional information from Windows endpoints can be collected at no extra cost. This data primarily covers patching details, making it highly valuable.

3.2.6.3. Agent-Based Logging

Where deeper insight is required, such as detailed performance metrics, event logs, or application-level diagnostics, an endpoint-based monitoring agent can be deployed to Cloud PCs. This approach provides granular visibility into CPU, memory, disk, network performance, and operating system events that native cloud reporting alone does not expose. However, this capability must be implemented with clear intent and defined use cases, as it introduces additional considerations, including:

- Increased data ingestion and storage costs
- Additional operational overhead for agent lifecycle management
- Potential impact on Cloud PC performance if not carefully configured

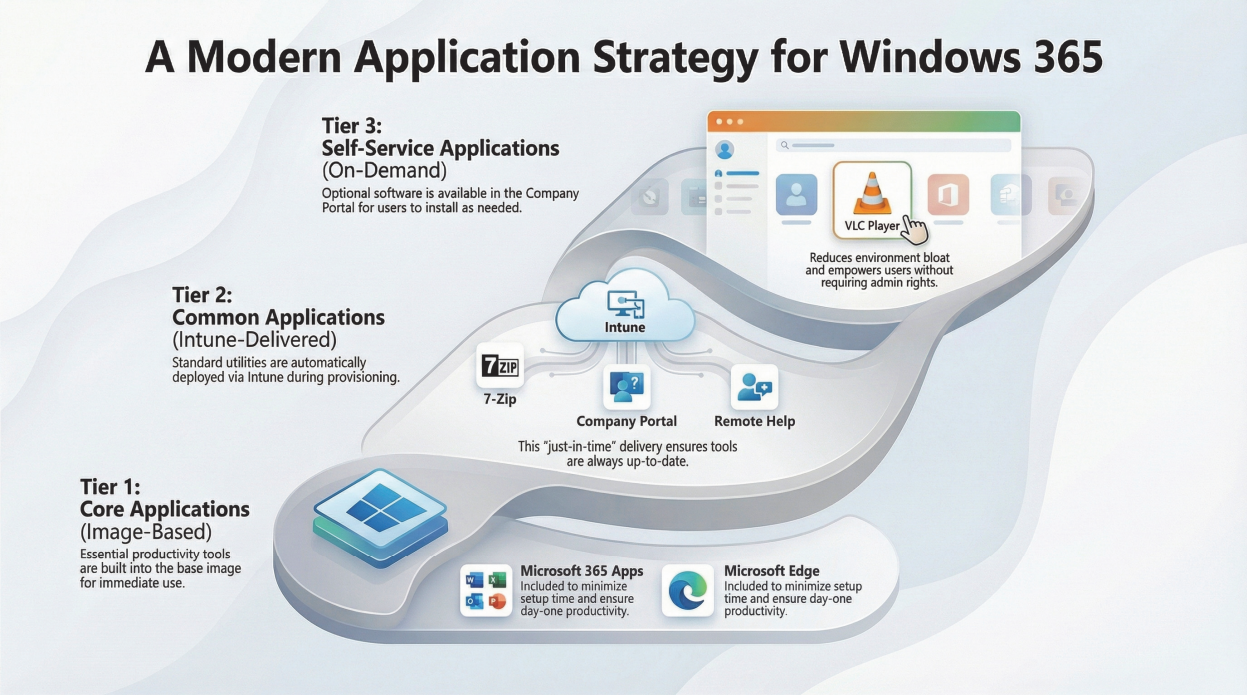
AS A GUIDING PRINCIPLE, ENHANCED MONITORING MUST BE PURPOSE-DRIVEN, ACTIVATED ONLY WHEN SPECIFIC OPERATIONAL, SECURITY, OR COMPLIANCE REQUIREMENTS JUSTIFY THE ADDED COMPLEXITY AND COST.

3.2.7. Application Management

The application delivery strategy for the Windows 365 environment prioritises automation, consistency, and user empowerment. By moving away from traditional, manual, resource-intensive imaging processes, the solution ensures that the Information Worker persona has immediate access to a secure, productive toolkit. Below is a catalogue of the applications for the proof of concept.

Application	Deployment Method	Notes
Microsoft 365 Apps	Pre-installed in the gallery image	Updated via Microsoft 365 CDN (Monthly Enterprise Channel). Included in Microsoft-optimised image.
Microsoft Edge	Pre-installed in the gallery image	Managed via Intune policies (e.g., default homepage, bookmarks, extension control).
Microsoft Teams	Gallery image (Autopatch-managed)	Auto-update via the Teams update channel; configure for AV optimisation on Cloud PC.
Remote Help	Intune Win32 app	A license is required for IT support staff. Recommended for helpdesk support in Zero Trust environments.

Company Portal	Microsoft Store app (Winget)	Enables user self-service software installation; must be targeted to all Cloud PCs.
7-Zip	Intune Win32 app (.intunewin package)	Silent installation during provisioning. Include detection rules for installation verification.
VLC Media Player (UWP)	Available in Company Portal (optional)	Optional app for training videos. Delivered via Microsoft Store with user-initiated install.



The architecture utilises a tiered "Modern Application Delivery Model" to manage the software lifecycle, categorising applications into three distinct phases of delivery:

- **Core Applications (Image-Based):** To minimise initial setup time, essential productivity tools like the Microsoft 365 Apps and Microsoft Edge are included directly within the Microsoft-optimised gallery image.
- **Common Applications (Intune-Delivered):** Standard line-of-business and utility applications, such as 7-Zip, Company Portal, and Remote Help, are deployed automatically via Microsoft Intune as part of the initial provisioning process. This "just-in-time" delivery ensures these tools are always up to date at deployment time.
- **Self-Service Applications (On-Demand):** To reduce environment bloat and helpdesk tickets, optional applications, such as VLC Player, are made available through the Company Portal. This allows users to install approved software on demand without requiring local administrative rights.

Strategic Application Principles

- **Browser-First Productivity:** Microsoft Edge is established as the primary enterprise browser, leveraging Chromium for high performance and deep integration with Entra ID for Single Sign-On (SSO) and Conditional Access.

- **Cloud-Native Servicing:** Applications are maintained through continuous cloud-based update channels, such as the Monthly Enterprise Channel for Microsoft 365, ensuring security patches are applied automatically without administrative intervention.
- **Unified Packaging:** Where applications are not available in the Microsoft Store, they are packaged as Win32 apps (typically using .intunewin format) to ensure secure and reliable delivery via the Intune Management Extension.
- **Look for Modern Apps:** Modern apps are more easily installed and upgraded than traditional Win32 applications. You can rely on Intune to keep these apps up to date.
- **Repackage When Needed:** Repackaging everything might be the instinct, but the packager has to account for the time to research, package, test and deploy an application. Usually, five devices are a good starting point.

3.2.7.1. Modern Applications (Windows Store)

As software vendors transition to modern application formats, the Microsoft Store (integrated with Intune) is the primary channel for consumption.

- **Deployment:** These applications require no manual repackaging. They are synchronised via Intune and published directly to the Company Portal app.
- **User Impact:** While initial communication may be required to introduce the Company Portal, this approach simplifies the long-term user experience by providing a single, trusted location for all software needs.

3.2.7.2. Win32 Applications (Legacy and Desktop)

Applications not available in the Microsoft Store require manual packaging to be compatible with Windows 365 and Intune. This process requires several phases and involves administrators in preparing and deploying application installations. A typical application packaging process can be summarised as follows:

Most applications are wrapped in an .intunewin file, a secure archive that contains the installation files and an installation script (typically PowerShell or Batch).

- **Challenges:** Win32 installers can be unpredictable. Success depends on deep technical knowledge of the specific software. Packagers often must build detection methods so that Intune can determine whether the application is present on the device.
- **Strategy:** For an extensive application portfolio, IT must partner with "Power Users" or departmental experts to validate installation behaviours and configurations.

The application must then be uploaded to Intune, which provides the installation files and parameters. The administrator will then work with testers to verify that the application installs and runs by publishing it.

Users either trigger the software installation or it is required, meaning the software is “pushed” to the machine for testing. Once some confidence is gained, the application can be made available to a broader community.

3.2.7.3. Browser Applications

Microsoft Edge (Chromium-based) is the standard enterprise browser for Windows 365 Cloud PCs. It is selected for its modern performance, high compatibility, built-in security controls, and tight integration with Microsoft 365 and Microsoft Entra ID. Standardising on Edge simplifies browser governance, enhances endpoint protection, and reduces fragmentation across the environment.

- **Compatibility and Performance:** Microsoft Edge leverages the same rendering engine (Chromium) as Google Chrome, ensuring broad compatibility with internal and external web applications, including those that rely on modern HTML5, CSS3, and JavaScript standards. It supports the complete Chrome extension ecosystem, providing feature parity with Chrome while enabling centralised extension management via Intune policies.
- **Enterprise Security Controls:** Edge integrates with Microsoft Entra ID to support Single Sign-On (SSO), Conditional Access, and Application Protection Policies (APP). These controls help ensure that access to cloud apps is authenticated, compliant, and protected against data leakage. Sensitive sessions can be isolated using Microsoft Defender Application Guard, Windows Sandbox, or Hyper-V-based containers to protect the host OS from untrusted content. Additionally, SmartScreen filtering and built-in tracking prevention enhance user safety during browsing.
- **Legacy Application Support:** For legacy web applications that require Internet Explorer components, such as ERP systems like JD Edwards (JDE), IE Mode in Edge enables seamless compatibility without needing a separate browser.

  Administrators can configure Enterprise Site Lists via Intune to automatically open designated URLs in IE Mode, ensuring user productivity while maintaining a secure and managed browsing environment.
- **Deployment and Configuration:** Microsoft Edge is pre-installed in the Windows 365 gallery image. Intune is used to manage Edge settings via configuration profiles, including the default homepage, startup behaviour, bookmarks, extension allowlist and blocklist, and browser update cadence. To ensure a consistent user experience and policy compliance, Edge is set as the default browser via Intune policies during initial provisioning. Browser telemetry and usage analytics can be monitored via the Microsoft Edge management portal.
- **Update Management:** Edge follows a frequent release cycle and is updated automatically unless managed otherwise. For environments enrolled in Windows Autopatch, browser updates are delivered via Microsoft's progressive rollout model, starting with test devices before scaling to production. This reduces the risk of regressions while maintaining a strong security posture.

3.2.7.4. Microsoft 365 Apps

Microsoft 365 Apps for enterprise (formerly Office 365 ProPlus) are automatically deployed to all Windows 365 Cloud PCs as part of the standard productivity stack. This includes core applications such as Word, Excel, PowerPoint, Outlook, and OneNote.

While Teams has separate servicing, it still falls under the Autopatch umbrella of policies and management. The deployment strategy ensures fast provisioning, consistent configuration, and continuous updates to support a secure and productive user experience.

- **Streamlined Deployment:** Microsoft 365 Apps are delivered through the Windows 365 gallery image. This cloud-native approach eliminates the need to package or

manage local installation media and ensures that every user receives the latest version in the image, reducing Cloud PC provisioning time.

- **Automatic Updates and Channel Management:** Updates are managed through the Monthly Enterprise Channel (MEC), which balances timely feature delivery with stability. This channel is configured using Microsoft Autopatch. Autopatch-managed environments further benefit from automated update health monitoring and staged rollouts, reducing the risk of disruptions due to bugs or regressions.

- **Security Hardening and Policy Enforcement:** Microsoft 365 Apps are secured using the Microsoft 365 Apps Security Baseline, a collection of pre-configured settings recommended by Microsoft to reduce exposure to known attack vectors. These policies cover macro behaviour, external content, ActiveX, add-ins, privacy settings, and legacy authentication mechanisms. The baseline is enforced via Intune configuration profiles and can be customised to meet organisational compliance requirements.

- **Licensing and Activation:** Users are automatically licensed for Microsoft 365 through group-based license assignment in Microsoft Entra ID. Activation is tied to the user's Entra ID credentials and supports SSO and Shared Computer Activation (SCA) to ensure proper license consumption across multiple virtual environments. This model enables seamless onboarding and supports scenarios where a user may access multiple Cloud PCs (e.g., in disaster recovery or training environments).

- **Cloud Integration and Data Protection:** Microsoft 365 Apps are fully integrated with OneDrive for Business and SharePoint Online. Known Folder Move (KFM) is configured to redirect user data (Desktop, Documents, Pictures) to OneDrive, ensuring files are backed up and available across sessions and devices. This integration also facilitates secure collaboration and enables advanced security controls such as Data Loss Prevention (DLP) and Microsoft Purview Information Protection.

3.2.8. Look and Feel

The "Day One" Experience

The user connects to Windows 365, where the device uses its layout configured from the image. By default, Windows 365 Cloud PCs are deployed from an image optimised for their role.

User Empowerment and Personalisation

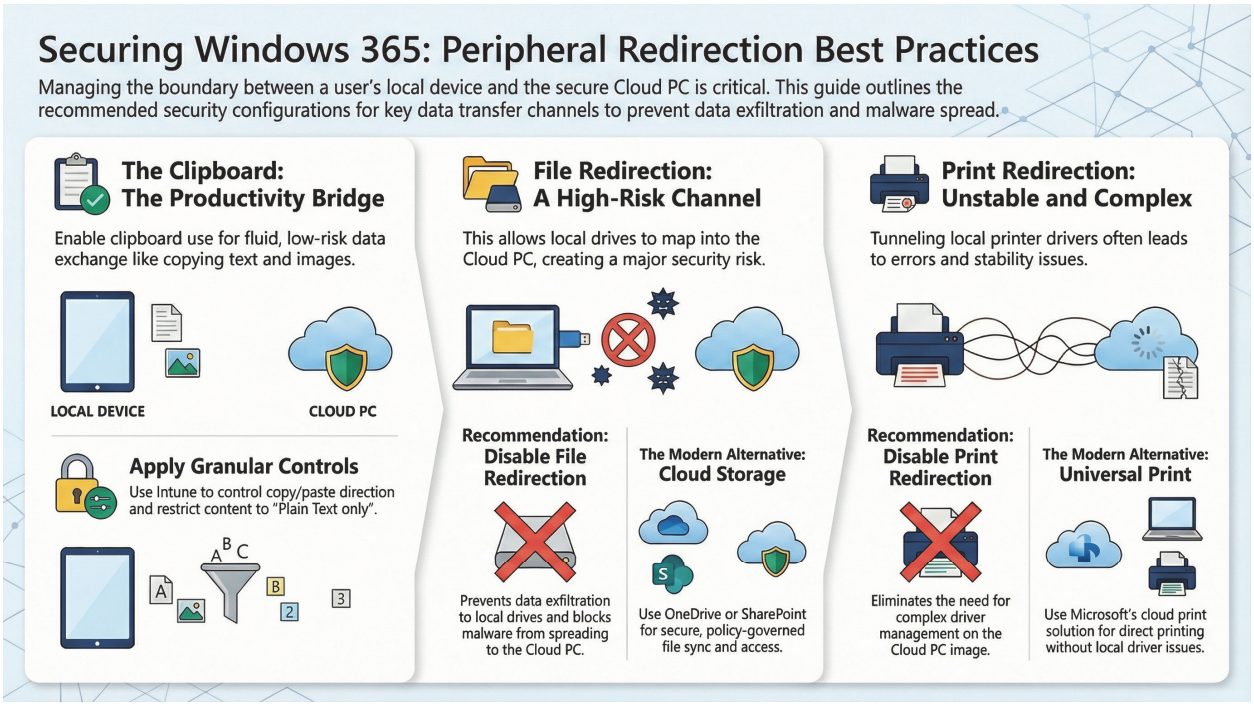
Unlike traditional "locked-down" environments, this implementation utilises the "Apply Once" logic, where, after provisioning, the user can configure the device as desired.

> **Initial Deployment:** The corporate layout is fine-tuned during the initial provisioning or first login.
>
> **Benefit:** This approach eliminates the common frustration of "UI resets," where user customisations are wiped during every policy sync or reboot, fostering a sense of ownership over their digital workspace.
>
> **Design Governance**
>
> By providing an orderly baseline, the organisation ensures that support documentation and training materials remain accurate (e.g., "Open the Edge icon pinned to your taskbar"). This consistency reduces helpdesk tickets related to "missing" applications while still allowing power users the flexibility to optimise their own workflows.

3.2.9. Clipboard, File, and Print

Managing the boundary between unmanaged local endpoints and the secure Cloud PC is critical for preventing data exfiltration and lateral movement. This section details the configuration of key data transfer channels, focusing on restricting physical device redirection (drives and printers) while

maintaining essential user workflows through granular clipboard controls and modern cloud alternatives.



3.2.9.1. The Clipboard: Facilitating Fluid Productivity

The clipboard serves as the primary bridge for "low-risk" data exchange. In a Windows 365 environment, enabling the clipboard allows users to copy and paste text, images, and formatted content between their local device and the Cloud PC.

Configuration Logic: Unlike file redirection, clipboard data is transient and typically limited in size. It is essential for workflows that involve referencing local notes while working in cloud-based enterprise apps.

Granular Control: Within Microsoft Intune, administrators can further refine this by:

Directionality: Allowing copy-paste from Cloud PC to local, but blocking local to Cloud PC (or vice versa).

Content Type: Restricting the clipboard to "Plain Text only" to prevent the transfer of potentially malicious scripts or large image files.

3.2.9.2. File Redirection: Protecting the Corporate Perimeter

Disabling file redirection (Drive Redirection) is a critical security posture. When file redirection is enabled, the endpoint's local drives appear as mapped network drives within the Cloud PC session.

Why Disable It?

Data Exfiltration: It prevents users from moving sensitive corporate data from the Cloud PC's managed storage to an unmanaged local disk or USB drive.

Malware Protection: It closes a common vector for "lateral movement," where ransomware on a compromised local endpoint could encrypt files stored within the Cloud PC.

The Modern Alternative: Since the Cloud PC is on a Microsoft-hosted network, users must utilise OneDrive for Business or SharePoint. These services synchronise data in the cloud, ensuring that files are scanned for threats and governed by Data Loss Prevention (DLP) policies, regardless of which device the user is logged in to.

3.2.9.3. Print Redirection: Moving Toward "Paperless" Cloud

Traditional printer redirection attempts to "tunnel" a local printer driver through the RDP stream. This often leads to driver mismatch errors and stability issues.

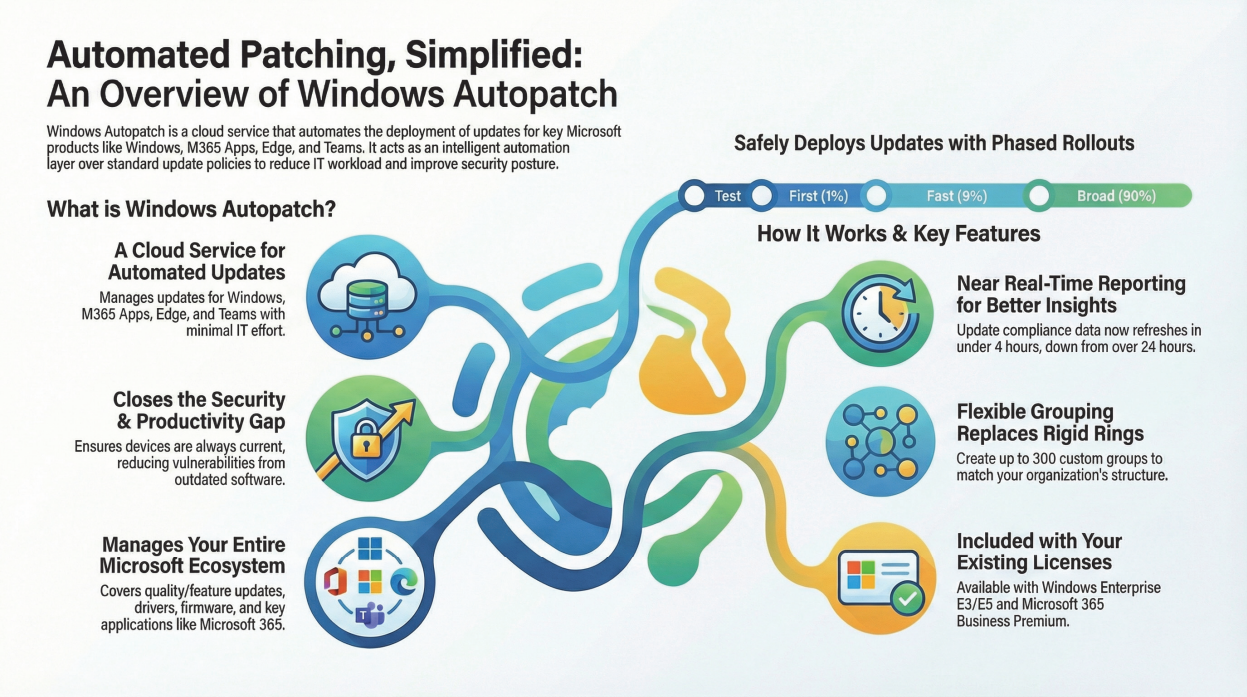
Architecture Strategy: Disabling print redirection eliminates the need for complex driver management on the Cloud PC.

Universal Print: If printing is an absolute requirement, the recommended approach is Microsoft Universal Print. This cloud-based print solution allows the Cloud PC to print directly to a network-attached printer over the internet (via the Microsoft-hosted network) without requiring a direct connection to the local endpoint's hardware.

3.2.10. Servicing

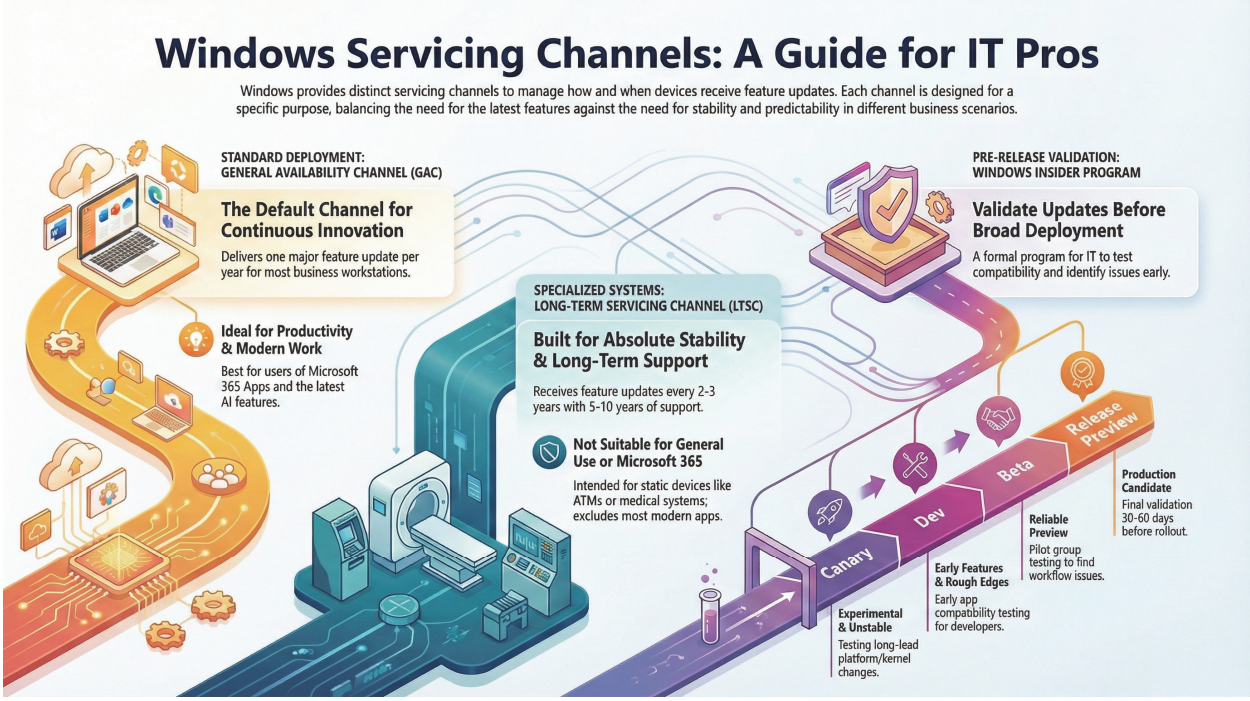
To maintain a secure, stable, and up-to-date Cloud PC environment, all servicing processes follow an "evergreen" model aligned with Microsoft's modern management strategy. This section outlines how updates are delivered and managed across the core components: Windows, Microsoft 365 Apps, Edge,

Teams, and management services.



3.2.10.1. Windows as a Service

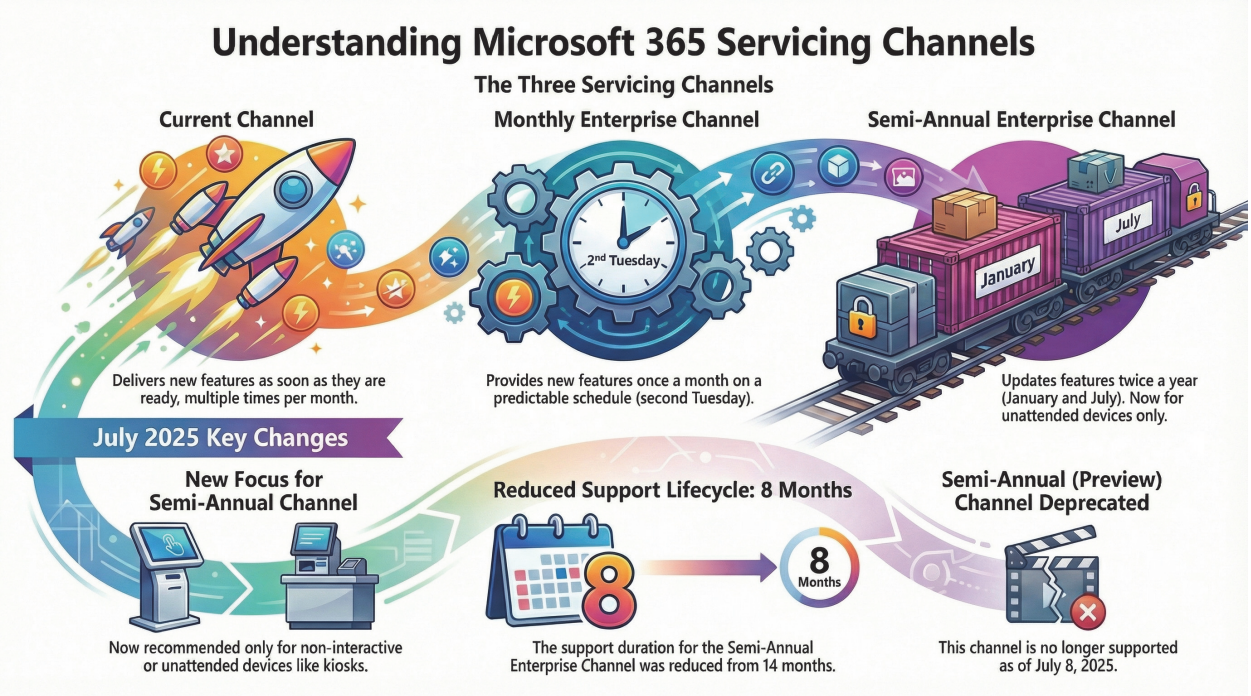
Windows 365 is maintained through a continuous delivery model known as Windows as a Service (WaaS). The dynamic nature of the Windows ecosystem requires a servicing strategy that is both agile and automated to ensure maximum compatibility and stability with Windows, Intune, Microsoft 365 and the Windows 365 service.



To meet these requirements, this design utilises Windows Autopatch as the primary servicing method. Built on Windows Update for Business (WUfB), Windows Autopatch is the industry-leading approach to modern endpoint management. It removes the manual burden of updating ring orchestration by automatically managing deployments, monitoring device health, and pausing updates if issues are detected. By adopting Autopatch, this design ensures the environment remains secure and compliant with minimal administrative overhead.

3.2.10.2. Microsoft 365 as a Service

Before introducing Autopatch, let's quickly review servicing channels for Microsoft 365. In July 2025, support changes were introduced, but for Windows 365 information workers, they will likely use the Monthly Enterprise Channel regardless of whether Autopatch manages Microsoft 365 updates. For reference, this infographic summarises the current state of Microsoft 365 servicing channels.



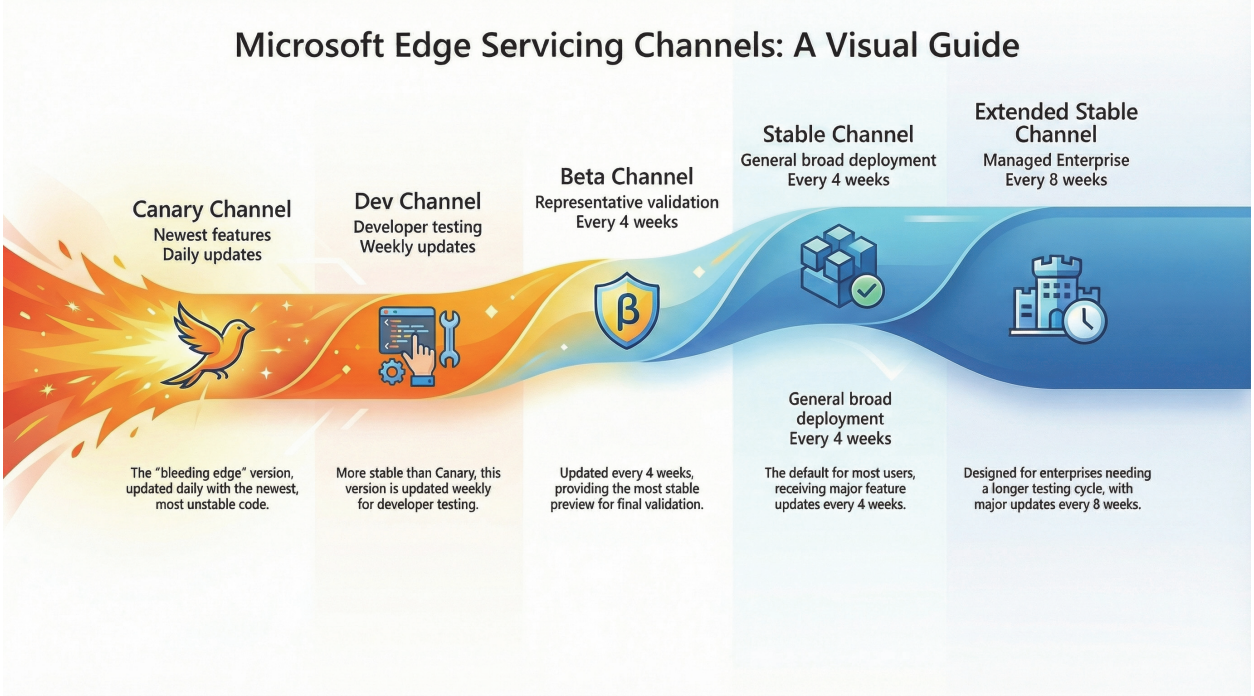
Beyond the operating system servicing, this design leverages Windows Autopatch to provide a unified update motion for the entire Microsoft productivity stack, including Microsoft 365 Apps for enterprise, Microsoft Edge, and Microsoft Teams. By extending the same automated ring-based logic to these applications, the service ensures that the productivity environment is consistently patched without requiring separate administrative workflows or manual intervention in the Microsoft 365 Apps admin centre.

For Microsoft 365 Apps, the service targets the Monthly Enterprise Channel (MEC) explicitly, aiming to keep at least 90% of eligible devices on a supported version. This approach balances the need for rapid security patching with the requirement for environmental stability. Updates are orchestrated through the same deployment rings used for Windows quality updates, allowing for early detection of potential application

compatibility issues in the Test and First rings before reaching the broader user population. This consolidated management model effectively "closes the security gap" for the entire endpoint, ensuring that both the OS and the core productivity tools are hardened against evolving threats simultaneously.

3.2.10.3. Edge as a Service

Edge offers service channels for different use cases. I often don’t see Edge updates being managed unless Autopatch is already active. Here is a quick overview of Edge servicing.



For Microsoft Edge, this design utilises the Windows Autopatch integration to automate browser servicing across the fleet. Instead of manually creating and targeting complex Settings Catalogue policies for browser channels, Windows Autopatch takes ownership of the Stable Channel delivery, ensuring that devices benefit from Microsoft’s progressive rollout model. By staggering the release of browser updates, the service can detect and mitigate potential web-app compatibility issues before they impact the broader organisation.

Devices placed within the Test ring are automatically moved to the Beta Channel, providing a critical early-warning system for the IT team to validate internal web applications against upcoming Edge releases. For the remainder of the environment, Autopatch enforces a consistent update cadence, checking for updates every few hours to ensure critical security fixes are applied rapidly. This approach significantly hardens the primary gateway to the web, "closing the security gap" by ensuring that the browser, often the most targeted application on an endpoint, is always running the most secure and performant version without requiring administrative intervention.

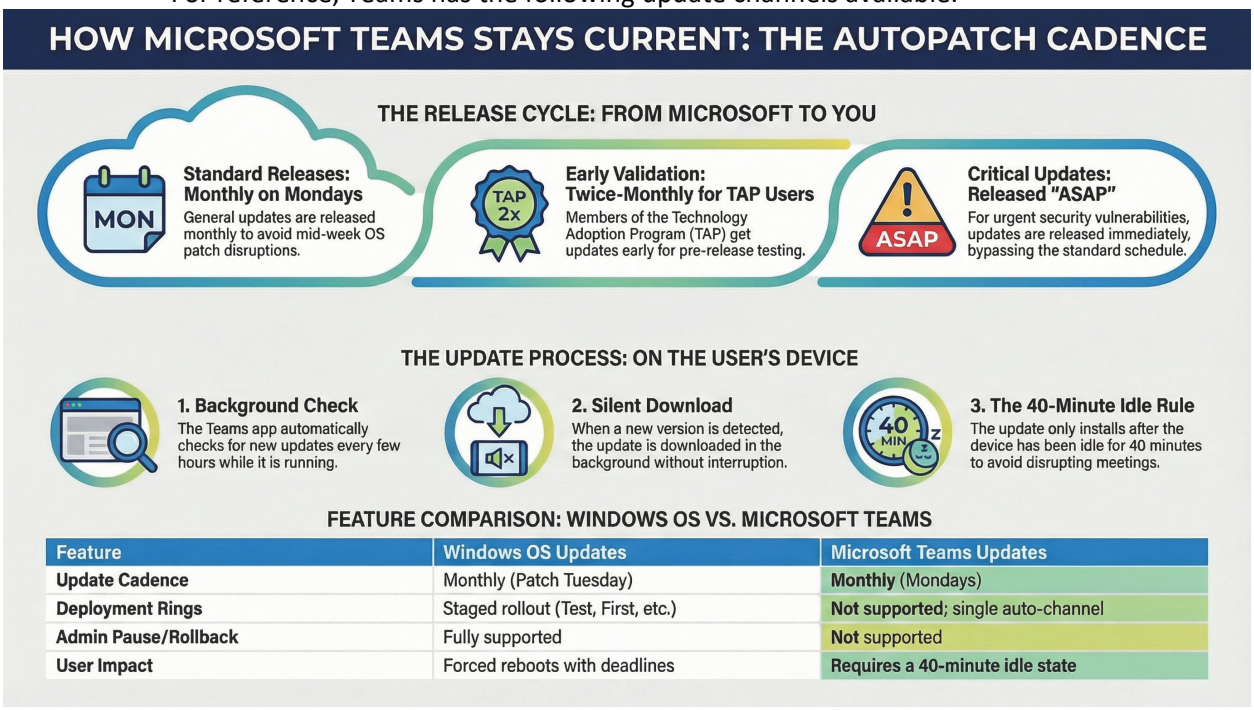
Why this supports the Windows 365 design:

- **Reduced Complexity:** It removes the need for manual "Target Channel Override" or "Update Policy" configurations in Intune.

- **Safety First:** It highlights the progressive rollout and the use of the Beta Channel for testing, which shows a mature approach to risk management.
- **Security Posture:** It frames browser patching as a critical security component, not just a "software update."

3.2.10.4. Teams as a Service

For Teams, there are many update channels available, but most are for specialised cases. For reference, Teams has the following update channels available.



This design utilises Windows Autopatch to ensure that Microsoft Teams remains current through its standard, automated update channel. Unlike the manual targeting required for legacy application deployment, Windows Autopatch allows eligible Cloud PCs to benefit from the native self-updating behaviour of the Teams service.

- **Standard Update Channel:** Teams is configured to check for updates every few hours in the background automatically. This ensures that users receive the latest features and security patches without IT intervention.

- **Idle-Time Installation:** To prevent work interruptions, Teams downloads updates silently and waits for the computer to be in an idle state (typically for at least 40 minutes) before completing the installation.

- **Service Monitoring and Support:** While Windows Autopatch does not directly pause or resume Teams updates, the service monitors update health across the fleet and provides official Microsoft support for any systemic update issues.

- **Windows 365 Optimisation: Maintaining the latest version of Teams is critical for Cloud PCs to leverage performance optimisations**, such as WebRTC-based peer-to-peer streaming, which ensures high-quality audio and video rendering.

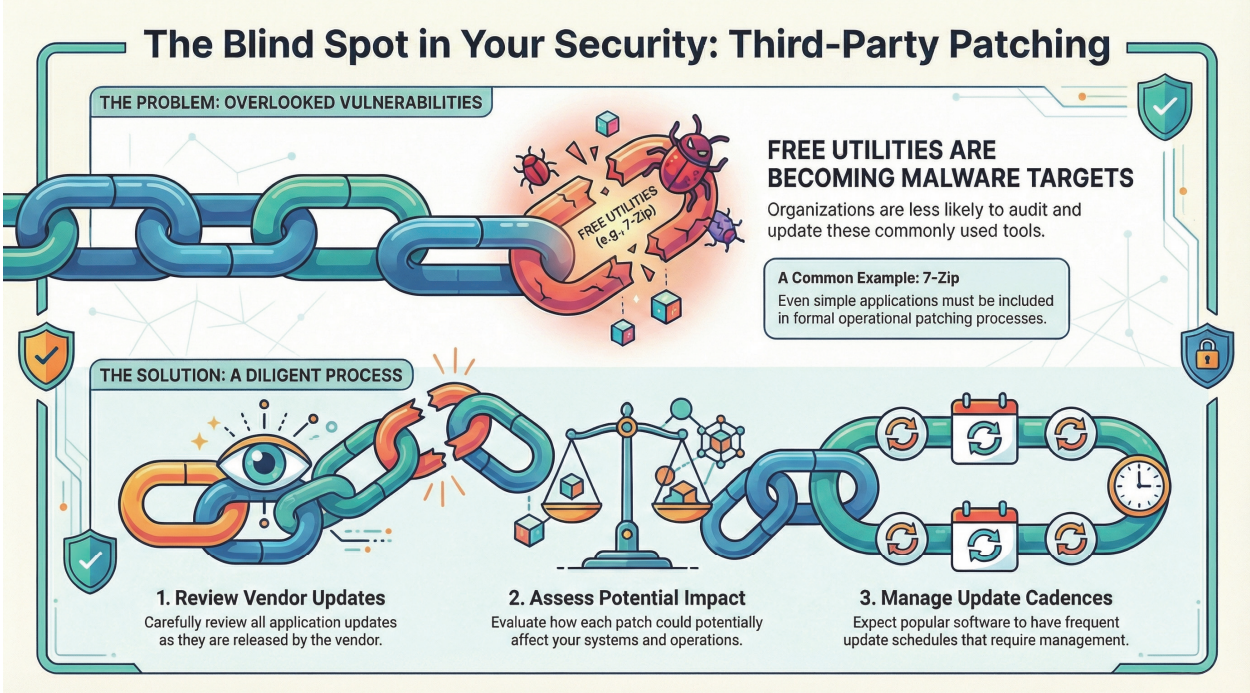
This model effectively "closes the security gap" by ensuring that the primary collaboration tool always runs a supported, hardened version alongside the rest of the Microsoft 365 productivity stack.

3.2.10.5. Modern Application Servicing

Windows is increasingly reliant on the Windows Store infrastructure to maintain modern applications on Windows devices, and completely disabling or removing the store is a poor decision for administrators. To support many of the contemporary applications that come with Windows 11 and some of the operating system components, the store will not be fully disabled.

3.2.10.6. Third Party Applications (Win32)

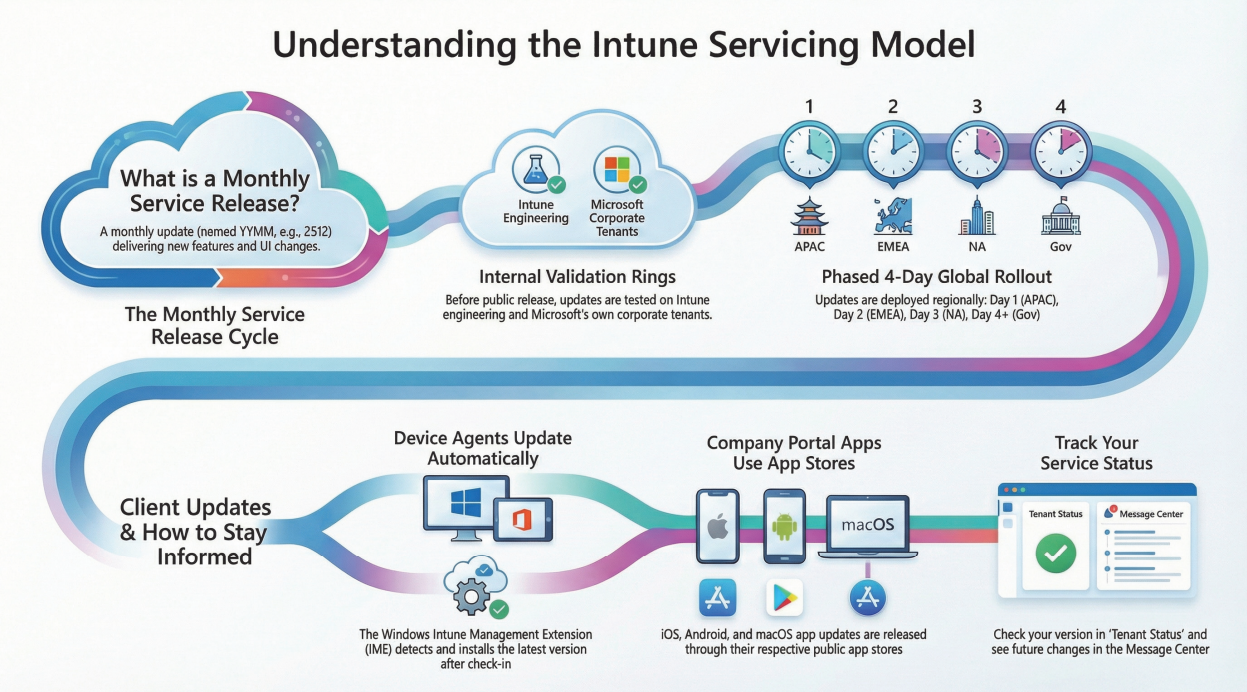
Third-party application patching is limited to 7-Zip, but it must be part of operational processes. Often-overlooked free utilities are becoming targets for malware because organisations are less likely to audit and update them.



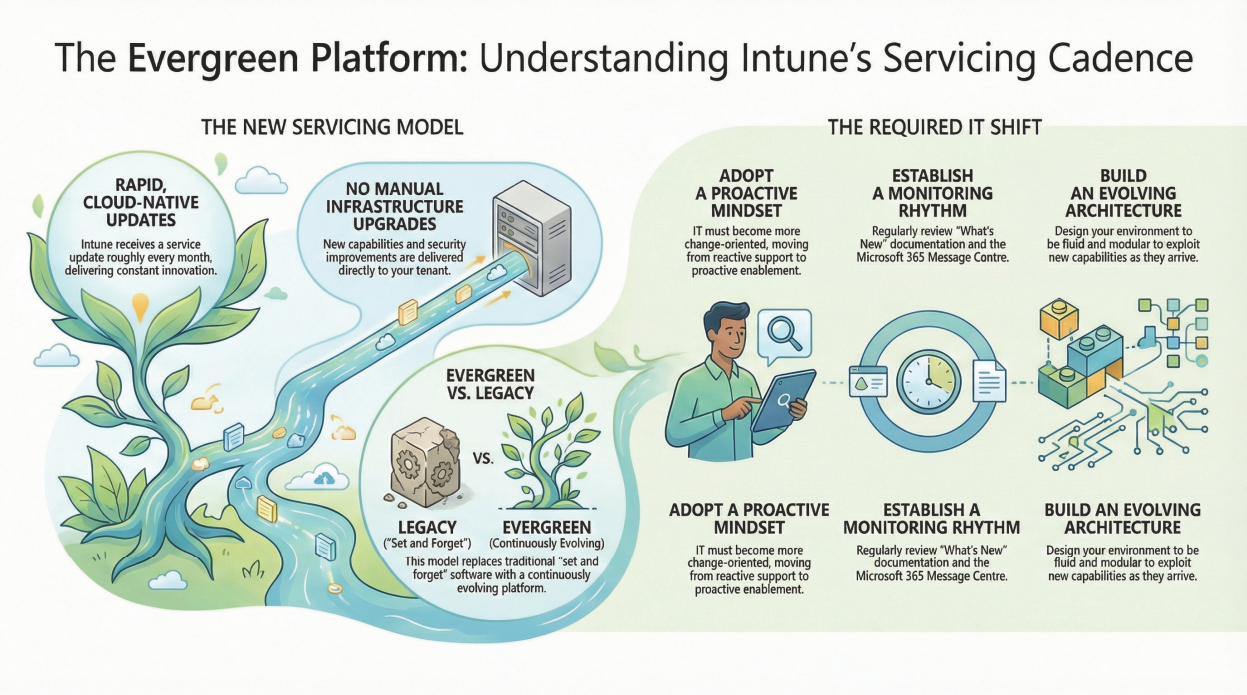
Tackling this challenge requires diligence to review the vendor-provided application updates and assess their potential impact. Expect more popular software titles to have frequent update cadences that must be managed.

3.2.10.7. Management as a Service

Microsoft Intune operates on a rapid, cloud-native servicing model that fundamentally changes how organisations manage endpoints. Because this portion of the solution is Microsoft-specific, it still requires understanding, as it impacts operations.



Unlike traditional on-premises software that relies on multi-year release cycles, Intune receives a service update roughly every month. This means new capabilities, security improvements, and UI enhancements are delivered directly to your tenant without requiring manual infrastructure upgrades. This constant stream of innovation ensures you are always running the most modern version of the tool, but it also requires a shift in how IT teams monitor and validate their management environment.



The Shift to Continuous Servicing

Part of a successful servicing strategy is staying on top of these service changes to help formulate a cohesive strategy for your environment. Because the platform is evergreen, the traditional "set and forget" mentality is no longer viable. Instead, IT departments must become more change-oriented, establishing a rhythm for reviewing the Microsoft Intune What's New documentation and the Message Centre in the Microsoft 365 admin centre. By proactively identifying which features can replace legacy workarounds or enhance security, you transform IT from a reactive support centre into a proactive business enabler.

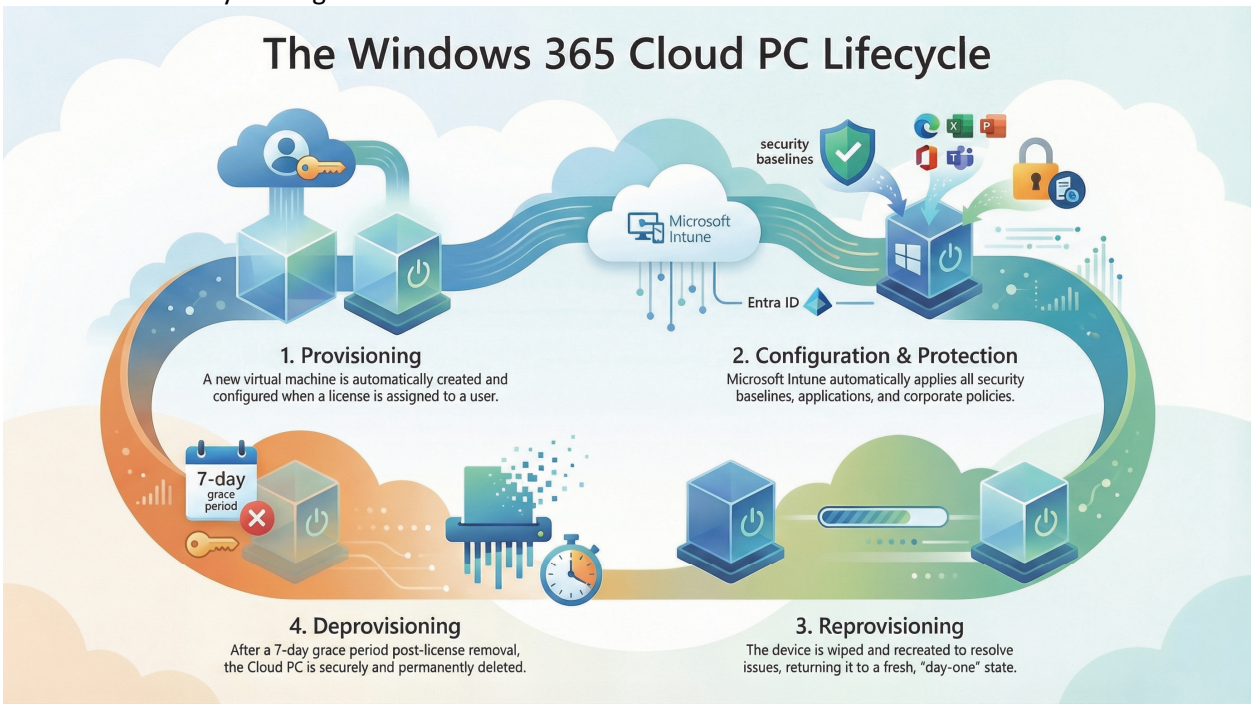
Building an Evolving Architecture

To succeed with cloud services, your technical architecture must be as fluid as the service itself. Exploiting new technical capabilities, such as migrating from GPOs to the Settings Catalogue or adopting new Windows 365 workflows, requires an ever-evolving architecture. This means designing your Intune environment with modularity in mind, allowing you to replace older management methods with newer, cloud-optimised ones as they become available. Embracing this "permanent beta" state enables your organisation to remain agile, secure, and competitive in a rapidly evolving digital landscape.

3.2.10.8. Device Lifecycle Management

The lifecycle of a Windows 365 Cloud PC is a managed process that ensures virtual desktops are efficiently deployed, maintained, and retired. This lifecycle is typically categorised into several key phases: Provisioning, Management/Reprovisioning, and Deprovisioning.

The Cloud PC Lifecycle Stages



Phase 1: Provisioning
The provisioning phase is the initial stage where a personalised virtual machine is automatically created and configured for a user. This process is triggered when an administrator assigns a Windows 365 license to a user and adds them to a Microsoft Entra ID group targeted by a provisioning policy. During this stage, the Windows 365 service orchestrates the creation of the VM, joins it to the network (either a Microsoft-hosted network or an Azure Network Connection), registers it with Entra ID, and enrols it into Microsoft Intune. This ensures the device is "ready-to-work" as soon as the user logs in for the first time.

Phase 2: Configuration and Protection
Once a Cloud PC is provisioned, it is handed off to Intune for additional application installation and configuration. This not only ensures users can be productive after signing in but also provides a trustworthy workspace for using their work applications and data. Additionally, authentication for this Cloud PC using Entra ID is subject to its own configuration access policies.

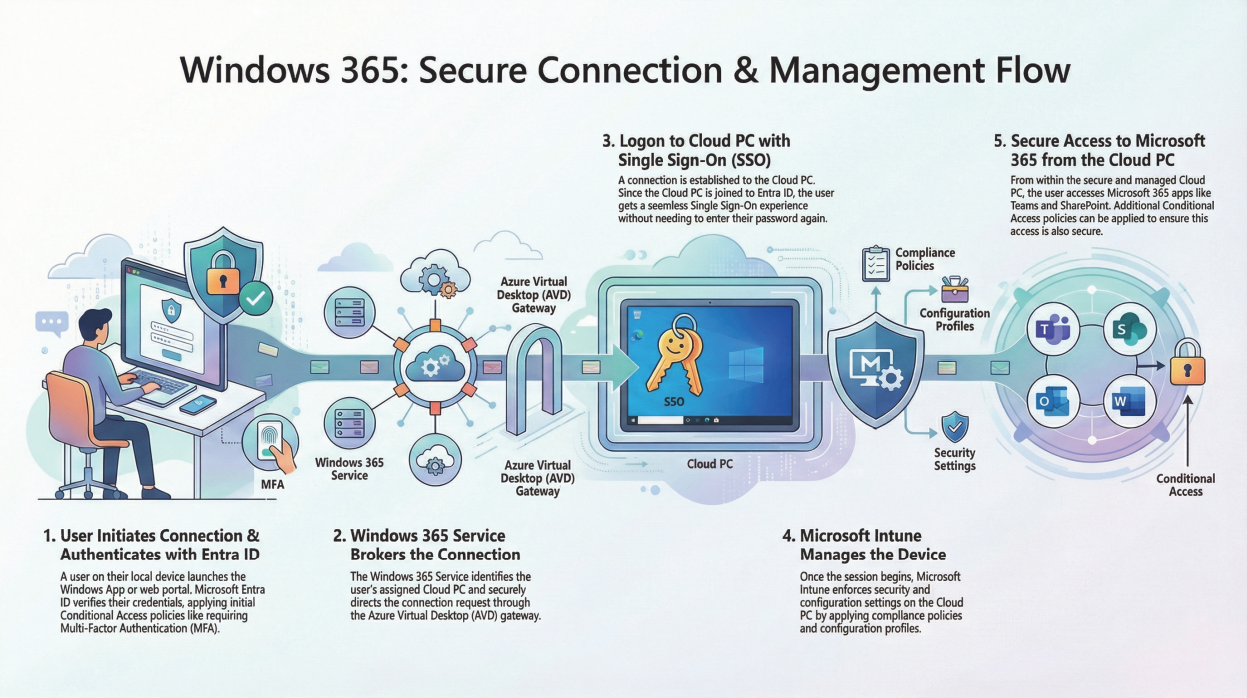
Phase 3: Reprovisioning
Reprovisioning serves as a maintenance or "reset" mechanism within the lifecycle, often used when a device is misbehaving or when significant configuration changes—such as a

new OS image or a change in the join type- need to be applied. When an administrator initiates reprovisioning, the existing Cloud PC is deleted, and a new one is created. It is important to note that this process wipes all user data, applications, and local customisations. It returns the user to a "day-one" state using the most current settings from the assigned provisioning policy.

Phase 4: Decommissioning (Deprovisioning)
The decommissioning or deprovisioning phase marks the end of the Cloud PC's lifecycle, typically occurring when a user leaves the organisation or no longer requires the resource. This phase is triggered when the user's license is removed or the provisioning policy is unassigned. Once triggered, the Cloud PC enters a seven-day grace period. During this window, the device remains accessible, allowing admins to recover data if necessary or restore access if the license was removed by mistake. After the grace period expires, the service automatically deletes the Cloud PC and its associated storage, permanently removing the resource from the environment.

4. Design Decisions and Conceptual Architecture

The conceptual architecture outlined below is intended to build on the core pillars of the Windows 365 solution, without delving into specific implementation details. This is a typical design in which Microsoft is responsible for much of the infrastructure, thereby simplifying the design. Conceptually, this is the Windows 365 end-user experience and management components.



To develop the design in detail, these sections will map user requirements to the technical requirements that drive the Windows 365 environment. These pillars are explained below and further explored throughout this section of the document.

1. **Entra ID Authentication**
   Using the Windows App, the end user can authenticate with their Entra ID credentials, which are further evaluated by conditional access.

2. **Windows 365 Service Broker Connection**
   When the user selects their Cloud PC in the Windows App, a connection is established to it. This allows a connection regardless of user location, provided an Internet connection is available.

3. **Log on to Cloud PC with SSO**
   Since the Windows App has a user token, it can make connecting to the Cloud PC seamless by avoiding duplicate credential prompts.

4. **Microsoft Intune Management**
   Intune uses a mostly agentless approach to managing Windows from the cloud. This platform installs patches and applications, configures settings, runs scripts, performs compliance checks, and more. It becomes the management platform for Windows 365 devices.

5. **Secure Microsoft 365**
   Entra ID and Conditional Access provide an additional layer of protection, ensuring that only compliant cloud PCs can connect to Entra ID-protected resources.

4.1. Windows 365 Knowledge Worker Technical Objectives

Each persona has a set of objectives for their work. For example, the technical objectives would be a simple list.

Windows 365 Knowledge Worker

1. Have access to a Cloud PC.
2. Use Entra ID
3. Use Intune
4. Applications
   - Microsoft 365
   - Edge
   - VLC player
   - Remote Help

4.2. Technical Scenarios

The Windows 365 pilot design, along with its supporting technology streams, introduces a range of new technical capabilities to the environment. This section summarises the key technical drivers behind implementing a Windows 365 Cloud PC for the chosen knowledge worker persona.

4.2.1. Windows 365 Technical Drivers

The following drivers are the key components driving the deeper technical elements of the Windows 365 design:

1. **Modern device lifecycle management**: Streamlining the provisioning, deployment, and retirement of Cloud PCs to reduce administrative overhead and improve user onboarding.
2. **Cloud-based device management**: Leveraging cloud-native tools to manage devices from anywhere, ensuring consistent policy application without the need for traditional on-premises infrastructure.
3. **A secure end-user computing platform**: Establishing a "Zero Trust" foundation by shifting the compute layer to the Microsoft Cloud, isolating corporate data from physical hardware.

Beyond these drivers, there are core technologies that power the modern Windows 365 platform:

4.2.1.1. Windows 365

In a modern Windows 365 design, the Windows 365 service acts as the primary catalyst for decoupling the operating system from physical hardware. By shifting the compute layer to the Microsoft Cloud, the service enables elasticity and high availability. By shifting the compute layer to the Microsoft Cloud, Windows 365 enables elasticity and high availability. It ensures the desktop environment is persistent, accessible from any location, and decoupled from the user’s physical device lifecycle. In effect, the traditional “PC” is transformed into a scalable cloud service.

It ensures that the desktop environment is persistent, instantly accessible from any location, and decoupled from the local endpoint lifecycle. This shift enables the organisation to deliver a standardised, high-performance Windows experience that is not constrained by the processing power or battery life of the user's physical device, effectively transforming the "PC" into a scalable cloud service.

Furthermore, Windows 365 shifts the security posture to a more virtualised model. Because data and applications reside entirely within Microsoft’s cloud boundary (not on local devices), Windows 365 becomes a central control point for preventing data exfiltration. This architectural choice also simplifies requirements at the physical access layer, allowing a range of endpoint hardware (from thin clients to personal laptops) without compromising corporate security. In essence, Windows 365 provides a secure, managed cloud environment for all user productivity.

4.2.1.2. Microsoft Intune

Microsoft Intune serves as the authoritative management engine within the Windows 365 design, providing the cloud-native framework required to oversee the entire lifecycle of the Cloud PC. By transitioning away from the localised constraints of Active Directory Group Policy and the infrastructure-heavy requirements of Configuration Manager, Intune introduces a more agile management model. It utilises Configuration Service Providers (CSPs) and the Settings Catalogue to enforce policies over the internet, ensuring that Cloud PCs remain compliant and secure regardless of the user’s physical location or the network they are utilising to connect.

In this architecture, Intune is responsible for the granular orchestration of the modern desktop, including the delivery of Win32 and Microsoft 365 applications, the enforcement

of security baselines, and the execution of proactive remediations. This engagement prioritises a cloud-only management strategy, deliberately excluding co-management to maintain a clean separation of duties. By establishing Intune as the sole management authority, the design eliminates the complexity of synchronising on-premises and cloud workloads, resulting in a streamlined administrative experience and a more resilient endpoint environment.

4.2.1.3. Windows Security

To establish a resilient and "Zero Trust" environment, the Windows 365 design leverages a suite of integrated Windows 11 security features orchestrated via Intune security baselines. These features are designed to protect the integrity of the Cloud PC, the user's identity, and the data residing in the Microsoft Cloud. By implementing these technologies, the design ensures that security is baked into the OS layer rather than treated as an add-on.

The following security technologies are core components of the hardening strategy:

- **Credential Guard:** Utilises virtualisation-based security to isolate secrets so that only privileged system software can access them, significantly mitigating the risk of pass-the-hash or pass-the-ticket attacks.
- **Secure Boot:** Ensures that the Cloud PC boots using only software that is trusted by the Original Equipment Manufacturer (OEM), preventing rootkits and boot-level malware from compromising the startup process.
- **Microsoft Defender SmartScreen:** Provides an early warning system against websites that may harbour phishing attacks or malware, and prevents the execution of unrecognised or malicious files.
- **Managed Disk Encryption:** While the underlying infrastructure utilises Azure Disk Encryption (ADE) to protect data at rest within the Microsoft data centre, Intune policies ensure that the virtualised disk environment remains compliant with organisational encryption standards without the overhead of traditional hardware-bound encryption.
- **Microsoft Defender Antivirus:** Acts as the primary defence against software threats, providing real-time protection, cloud-delivered behavioural analysis, and automated remediation of detected threats.
- **Windows Firewall:** Enforces granular network segmentation at the device level, controlling inbound and outbound traffic to ensure that only authorised communication occurs between the Cloud PC and the broader network.

4.2.1.4. Windows 11

For this design, Windows 11 Enterprise 25H2 serves as the baseline image. Utilising the latest feature update ensures that the environment supports the most recent architectural improvements in kernel security, virtualisation-based security (VBS), and integrated AI capabilities.

- Feature Parity: By starting with 25H2, we ensure full compatibility with the latest Microsoft Intune administrative templates and CSPs (Configuration Service Providers).
- Hardware Optimisation: 25H2 is optimised for the virtualised hardware specifications of Windows 365, particularly regarding vGPU acceleration and NPU (Neural Processing Unit) offloading for AI-enhanced background effects and system performance.

4.2.1.5. The "Dynamic Cloud PC" Philosophy

A core tenet of this design is that Cloud PCs must be treated as dynamic, evergreen assets rather than static infrastructure. Unlike traditional on-premises VDI, which often suffers from "image inertia," the Windows 365 environment is designed to scale with the service.

- **Zero Technical Debt:** By mandating the use of the latest OS version, we eliminate the need for complex "big bang" migration projects every few years. The environment stays in a state of continuous evolution.

- **Stateless Mindset:** This approach encourages a separation of the OS, the apps, and the data. By utilising OneDrive Known Folder Move (KFM) and Enterprise State Roaming, the underlying OS version can be updated, or the Cloud PC reprovisioned with minimal impact on the end-user experience.

4.2.1.6. Provisioning and Update Strategy

To maintain this dynamic state, the design utilises Marketplace Images rather than thick, custom-built "golden images."

- **Gallery Images:** We leverage the Microsoft-optimised gallery images for 25H2, which include pre-configurations for Microsoft 365 Apps. This ensures the OS is always patched to the latest security baseline during provisioning.

- **Autopatch:** Post-deployment, the "dynamic" nature is maintained through aggressive update policies. Cloud PCs are placed in "Fast" or "Broad" rings to ensure that, as Microsoft releases monthly quality updates and annual feature updates, the fleet moves forward automatically without manual intervention. Common applications such as Edge and Microsoft 365 use this mechanism to improve patch compliance.

4.2.1.7. Security and Compliance Benefits

Standardising on the latest OS version significantly reduces the attack surface.

- **Immediate Vulnerability Remediation:** Most modern exploits target legacy OS components. By staying on 25H2, we benefit from the latest mitigations against credential theft and memory-based attacks.
- **Compliance Alignment:** Maintaining the latest version simplifies reporting for regulatory frameworks, as the environment is always aligned with the Windows 11 General Availability Channel. We will use the latest available version of Windows 11 Enterprise. That version is the 25H2 release. As a rule, Cloud PCs must be dynamic and always use the latest operating system version.

4.2.1.8. Microsoft 365

As Microsoft 365 is our core productivity suite, its deployment and management must be handled with the utmost care. To ensure every installation is current and secure, we will leverage Intune's native cloud installation capability to deliver the most up-to-date Microsoft 365 suite at deployment.

Beyond the installation itself, we are introducing Microsoft 365 security baselines in Intune to establish a rigorous security configuration. This proactive approach hardens our modern devices against emerging threats and effectively mitigates risks that utilise Microsoft 365 as a primary attack vector.

4.3. Cloud and Identity

The integration of Windows 365 marks a transition from traditional on-premises infrastructure to dynamic, cloud-delivered services. This shift redefines identity management: where Active Directory once served as the primary authority, the rise of cloud-native application architectures now demands adopting cloud-native identities. By consolidating all user credentials in a centralised cloud identity provider (Microsoft Entra ID), IT can more effectively manage security posture and scale the desktop resources across the enterprise.

4.3.1. Cloud Services and Licensing

Currently, the organisation has broadly adopted cloud identity (Entra ID) and uses Intune for device management. This section will also cover cloud licensing, since it will be managed in the cloud using Windows 365 devices. An overview of the current state and key decisions is provided in the table below.

4.3.1.1. Current State

The following cloud services are currently in place.

Cloud Service	Business Area	Usage Scenarios
Entra ID	Company Wide	Cloud-based identity for Microsoft and third-party services.
Intune	Company Wide	Cloud-based mobile device management and mobile application management platform.
Microsoft Cloud Licensing	Company Wide	Used primarily for Microsoft 365 and some device licensing.
Microsoft IDs	Company Wide	Not managed, users are using personal IDs on some machines. Enabling personal email and OneDrive.

4.3.1.2. Decisions

This section outlines the foundational identity and management framework for the Windows 365 environment, with a focus on scalability, security, and automated administration.

4.3.1.2.1. All Cloud PCs will be natively joined to Entra ID.

Justification: Native Entra ID join is the recommended modern identity state for Windows 365. It eliminates the need for line-of-sight to a physical Domain Controller, simplifies provisioning, and provides a smoother Single Sign-On (SSO) experience. It also ensures that devices are managed entirely via modern authentication protocols.

Design Detail: No Hybrid Entra ID Join or local Active Directory dependencies will be included in the device provisioning workflow, reducing infrastructure complexity.

4.3.1.2.2. Create a dynamic Cloud PC Entra ID group

Justification: Using dynamic groups ensures that as soon as a Cloud PC is provisioned, it automatically receives the necessary configuration profiles, security baselines, and application deployments without manual intervention.

Implementation: The group will use a membership rule similar to:

(device.displayName -startsWith "CPC-")

Impact: This provides a reliable "catch-all" for policy targeting, ensuring zero-touch configuration for the lifecycle of the device.

4.3.1.2.3. Create assigned Cloud PC user group

Justification: Centralising the onboarding process into a single group membership simplifies administrative overhead. By nesting licensing, provisioning policies, and user settings in this group, IT can "onboard" a user simply by adding them to the group.

Design Detail: This group will be the primary target for:

- Windows 365 License assignment (via group-based licensing).
- Provisioning Policy (defining the region, image, and network).
- User Settings (defining local admin rights and PIT restore frequencies).

4.3.1.2.4. Make a group for Cloud PC administrators

Justification: This is the minimum required to administer the environment at this time. It will be used to grant administrators access to the pilot environment as full Intune administrators and local administrators on each Cloud PC.

Design Detail: This group will be the primary target for:

- Intune role assignment.
- Local administrator rights on cloud PCs.

4.3.1.2.5. Intune manages Windows 365

Justification: Windows 365 is a cloud-native service deeply integrated with the Microsoft Intune admin centre. Using Intune allows for unified management of

physical and virtual endpoints, providing a "single pane of glass" for application delivery, Windows updates, and security configurations.

Design Detail: Configuration will include Enrollment Status Pages (ESP) and proactive remediations to maintain the health of the Cloud PC fleet.

4.3.1.2.6. Implement conditional access policies

Justification: Conditional Access is the "Zero Trust" gatekeeper. By creating policies specifically for the "Windows 365" cloud app, the organisation can enforce stricter requirements for virtual desktops than for other SaaS apps.

Additional policies for Microsoft 365 applications help ensure the Cloud PC is in a trusted state before granting access to sensitive data. This will enable IT to maintain two separate gates while keeping them seamless to the end user.

Design Detail: Policies will likely include:

- **MFA Requirement:** Mandating multi-factor authentication for all scenarios.
- **Device Compliance:** Ensuring the connecting device (Cloud PC to M365) meets security standards.
- **Location-Based Access:** Restricting access to known corporate IP ranges or regions if required.
- **Phishing Resistant MFA:** All administrator accounts will require the use of phishing-resistant MFA.

4.3.1.2.7. Require M365 licensing

Justification: M365 E3: Provides the underlying Windows 10/11 Enterprise license rights required for VDI, along with the Intune and Entra ID P1 licenses necessary for management and security.

4.3.1.2.8. Require Windows 365 licensing

Justification: Assigns a specific compute resource (vCPU, RAM, Storage) to the user's Cloud PC.

Compliance Note: Users must have both licenses active to trigger the provisioning and login flows successfully. This will be done by adding them to the Cloud PC user group.

4.3.1.2.9. **Microsoft (personal) accounts are not permitted on Cloud PCs**

Decision: Users cannot use personal accounts for OneDrive, Windows or the Mail and Calendar apps.

Justification: This reduces the attack surface and helps prevent the leakage of sensitive data.

Impact: Users will have to use personal devices or a web browser to access services.

4.3.1.3. Decision Success Criteria

Decision Area	Key Decision	Success Criteria
Device Identity (Entra ID Join)	Join all Cloud PCs to Microsoft Entra ID natively.	100% Cloud PCs joined to Entra ID; no hybrid joins.
Device Grouping (Dynamic Group)	Use a dynamic Entra ID group with naming prefix logic.	All Cloud PCs appear in a dynamic group within 5 minutes of provisioning.
User Management (Licensed User Group)	Use a dedicated Entra ID group for Cloud PC licensed users.	Users receive a license and a provisioning profile upon joining the group.
User Management (Cloud PC Admin Group)	Use a separate Entra ID group for Cloud PC admins.	Admin users receive Intune and local admin rights automatically.
Endpoint Management (Intune Authority)	Intune will be the sole management authority.	All Cloud PCs report into Intune and apply ESP/profiles successfully.
Security (Conditional Access Policies)	Enforce targeted Conditional Access policies.	Conditional Access applied to all Cloud PCs and M365 apps; MFA and compliance enforced.
Licensing Requirements	Assign both M365 E3+ and Windows 365 licenses.	All users with Cloud PCs have both licenses assigned and provisioned correctly.
Microsoft Personal Accounts	Block personal Microsoft accounts on Cloud PCs.	No Cloud PCs show evidence of personal account logins (OneDrive, Mail, Store).

4.3.2. On-Premises Identity

4.3.2.1. Current State

Primary Directory Functional Level	Windows Server 2026
Federated?	Yes
Domain Controller Operating System	Windows Server 2025 LTSC
Using Entra Connect?	Yes
Cloud identity providers	Entra ID
Synchronisation method/tool	Entra Connect, Pass Thru Authent

4.3.2.2. Decisions

For the Windows 365 identity infrastructure, the following decisions have been made:

4.3.2.2.1. Users will not exist in Active Directory

Given the current infrastructure and project objectives, there is a clear opportunity to streamline the identity model for the Windows 365 deployment. The design's goal is to move to a cloud-native identity model to reduce technical debt and complexity, even though some on-premises infrastructure (like Active Directory) still plays a role (for example, in specific admin roles or legacy apps). Ideally, all remaining legacy identity dependencies will be eliminated in the

future state. By utilising Entra ID Join for these Cloud PCs, we eliminate the dependency on legacy on-premises domain controllers and the complexities of line-of-sight connectivity to the local network.

This shift to a cloud-only identity footprint significantly enhances the device's security posture. By removing the Cloud PC from the local domain, we reduce the lateral movement attack surface and eliminate risks associated with legacy authentication protocols such as NTLM and Kerberos. Users authenticate directly with Entra ID, enabling seamless application of Conditional Access policies, multi-factor authentication (MFA), and continuous access evaluation without the overhead of traditional domain services.

Furthermore, this "Entra-only" approach simplifies the management lifecycle. Since the device and the user exist exclusively in the cloud, there is no need for Hybrid Entra ID Join, which often introduces synchronization delays and troubleshooting complexity during the provisioning process. This design ensures that the Cloud PC is ready for use immediately upon assignment, providing a more responsive and resilient experience for the Information Worker persona while maintaining a strict boundary between cloud assets and the on-premises core.

Feature	Hybrid Entra ID Join	Entra ID Join (Cloud Only)
Identity Source	Synchronized (AD + Entra ID)	Cloud Native (Entra ID)
Domain Dependency	Requires On-Prem Domain Controller	No On-Prem Dependency
Network Path	Requires VNet with line-of-sight to AD	Direct Internet / Microsoft Hosted
Security	Supports legacy protocols	Modern Auth / Zero Trust focus
Provisioning Speed	Slower (Wait for AD sync)	Fast (Instant availability)

4.3.2.2.1. Microsoft (personal) accounts are not permitted on Cloud PCs

The decision to prohibit the use of personal Microsoft accounts on Cloud PCs is a prudent security measure that establishes a clear boundary between corporate and private data. By restricting authentication exclusively to managed Entra ID identities, the organisation ensures that all user activity remains within the governance of corporate security policies, such as Conditional Access and session monitoring. This restriction effectively mitigates the risk of unauthorised data exfiltration to personal OneDrive or Outlook accounts and prevents the

introduction of unmanaged synchronisation points. Maintaining this separation is essential for achieving a Zero Trust architecture, as it ensures that the Cloud PC remains a dedicated, secure workspace free from the "grey area" of mixed-use personal identities.

4.3.2.3. Decision Success Criteria

Decision Area	Decision / Standard	Decision Criteria	Success Criteria	Validation / Evidence
Primary Identity Source	Will not exist in Active Directory; users may exist cloud-only in Entra ID	Enables cloud-first onboarding and eliminates dependency on legacy directory services	Cloud PC users can be provisioned successfully without an AD object	Cloud PC provisioned successfully using Entra-only identity; user sign-in logs show cloud auth
Hybrid Identity Footprint	Entra Connect remains in place for environments that still sync identities, but Cloud PC does not depend on it	Avoids provisioning delays and troubleshooting caused by sync timing issues	Cloud PC provisioning works even during Entra Connect outages or sync delays	Provisioning logs show no dependency errors; tested by provisioning during paused sync
Federation / Authentication	Existing federated authentication remains supported (e.g., PTA), but Cloud PCs authenticate via Entra ID	Prevents the Cloud PC identity model from being constrained by federated availability	End-users can authenticate to Windows 365 even if on-prem DC access is unavailable	Authentication and access succeed using Entra ID conditional access signals
Domain Controller Dependency	Cloud PCs do not require line-of-sight to Domain Controllers	Eliminates reliance on network tunnels, VPNs, and legacy routing	Users can connect to Cloud PCs from any internet connection successfully	Users log in remotely without DC access; no “domain unavailable” errors
Join Strategy	Cloud PCs are Entra ID joined (Cloud Only), no Hybrid Entra Join	Removes technical debt, reduces provisioning latency, and improves Zero Trust posture	100% of Cloud PCs are Entra ID joined and show no hybrid join state	Entra ID device properties show Join Type = Entra ID Joined; Intune enrollment successful

Personal Microsoft Accounts	Personal Microsoft accounts are not permitted on Cloud PCs	Prevents unmanaged sync points, personal OneDrive exfiltration, and reduces attack surface	User cannot sign into Windows services / OneDrive / apps using personal accounts	Attempted sign-in is blocked; policy validation confirms restriction
Identity Boundary Control	Cloud PCs must use corporate Entra identities only for login and service access	Ensures identity governance, Conditional Access coverage, and auditability	All Cloud PC sign-ins are through managed Entra users; no consumer ID sign-ins	Entra sign-in logs show only managed identities; policy report confirms enforcement

4.4. Cloud PC and Provisioning

This section of the architecture document outlines the initial phase of the project: deploying and managing Windows 11 cloud PCs. The following topics address the Cloud PC specifications, operating system and provisioning profile for the information worker. The device personas and operating system requirements significantly shape the deployment solution's requirements. Each section outlines the key decisions for each component.

4.4.1. Devices

4.4.1.1. Requirements

Cloud PC Size: The following outlines the performance capabilities required for the Information Worker.

vCPU	RAM	Storage	Performance Tier	Use Case
2	8 GB	128 GB	Standard	Information worker

Windows Image: The image must be maintained by Microsoft and must include Microsoft 365 apps.
Networking: The solution must provide the easiest way to configure and maintain networking.
Physical Device: Users must be able to access the solution using a supported version of Windows 11 that can be a personal device.

4.4.1.2. Decisions

This section expands on the architectural design decisions for your Windows 365 Cloud PC specifications. These decisions prioritise scalability, ease of management, and alignment with Microsoft best practices for a cloud-native endpoint strategy.

4.4.1.2.1. Licensing and Performance Tiers

The selection of performance specifications is mapped to defined User Personas. For most knowledge workers, the 2vCPU / 8GB RAM specification is the baseline. However, for users requiring nested virtualisation or heavy multitasking, the 4vCPU / 16GB RAM tier is recommended. By committing to these specs early, the procurement process is streamlined, and licenses can be assigned immediately via Microsoft Entra groups.

4.4.1.2.2. Network Connectivity (Microsoft-Hosted)

By opting for a Microsoft-hosted network, the organisation adopts a "Zero Trust" ready posture. Traffic does not need to be backhauled to an on-premises data centre unless specific legacy line-of-business (LOB) applications require it. This decision reduces latency for SaaS applications and simplifies the "Provisioning Policy" configuration by eliminating Azure Network Connection (ANC) health checks for the VNet.

The geography for this design is in the Western United States; as a result, the closest Azure Geography is Azure West. The assumption is that user proximity is the primary factor, but other constraints may arise, such as applications and resources in cloud locations that are not local to the Cloud PC.

4.4.1.2.3. Physical Device Strategy

The solution must support users connecting from an unmanaged device using Windows 11 and the Windows App. BYOD devices are in scope to ensure that end-users have flexible access to their Cloud PC from a personal device when needed.

4.4.1.2.4. Image Strategy (Gallery vs. Custom)

To maintain an agile environment, this design utilises Microsoft Gallery Images. These images are updated monthly by Microsoft to include the latest security patches and versions of Microsoft 365 Apps.

- **Application Delivery:** Instead of baking apps into a custom image, all specialised software will be deployed as Win32 apps or MSIX packages via Microsoft Intune.
- **Benefits:** This "thin image" approach ensures that the provisioning process is faster and more reliable, as the underlying OS remains "clean" and supported directly by Microsoft.

4.4.1.3. Decision Success Criteria

Decision Area	Decision / Standard	Why This Decision Matters	Success Criteria	Validation / Evidence
Cloud PC Performance Tier	Standardise the Information Worker persona on 2 vCPU / 8 GB RAM / 128 GB SSD.	Provides the best balance between user performance and fixed monthly licensing cost.	Pilot users report responsive Teams + Microsoft 365 performance with no routine bottlenecks.	User feedback survey; performance telemetry (Teams call quality, CPU/memory utilisation)
Persona-Based Sizing	Cloud PC sizes must be mapped to defined	Prevents overspend on	Users are placed into the correct SKU tier	Persona → license mapping register;

	personas; power users may require higher SKU tiers. (e.g., 4 vCPU / 16 GB / 256 GB)	licenses while ensuring high-demand users do not experience degraded performance.	based on workload and do not require "emergency resizing".	provisioning validation results.
Network Strategy	Use Microsoft-hosted network (ALB) for pilot deployments.	Simplifies design and removes the requirement for an Azure subscription, VNet, VPN, or routing.	Cloud PCs are provisioned without ANC failures and connect reliably from any location.	Provisioning logs show no ANC dependencies; successful user connection tests.
Image Strategy	Use Microsoft-maintained Gallery Images, including Microsoft 365 Apps.	Ensures images remain evergreen, secure, optimised for Cloud PC, and reduces image maintenance overhead.	Cloud PC provisioning is consistent, and the OS image stays supported without custom patching workflows.	Provisioning policy image source shows Gallery; OS version consistent across pilot devices.
OS Baseline Standard	Standardise on Windows 11 Enterprise. (Latest Stable – 25H2)	Reduces technical debt and ensures compatibility with modern CSPs, baselines, and security features.	100% of Cloud PCs run Windows 11 25H2 with no drift.	Intune OS inventory reporting; Windows 365 portal version checks.
Device Group Targeting	Policies must target Cloud PCs using dynamic device groups driven by naming.	Supports "zero touch" configuration and avoids manual device targeting overhead.	Newly created Cloud PCs automatically receive configuration profiles, baselines, and apps.	Policy assignments show correct scope; deployment status is successful within the expected window.
Application Delivery Model	Use a thin image + Intune app delivery model. (not thick/custom images)	Improves provisioning reliability, speeds.	Mandatory apps deploy successfully during provisioning, and optional apps are	Intune deployment status; Company Portal availability validation.

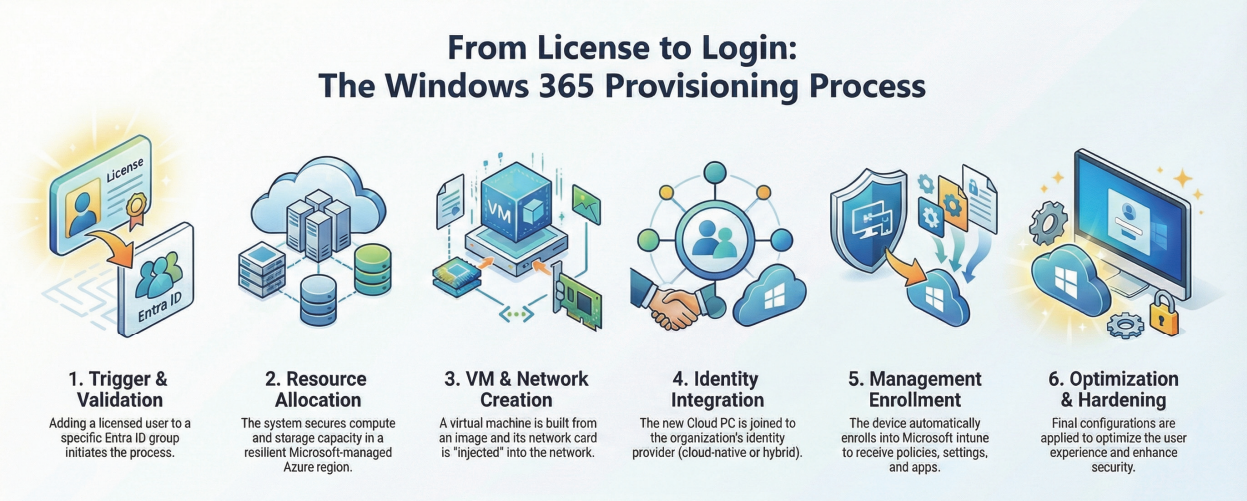
		deployments, and reduces image management complexity.	available via Company Portal.	
Cloud PC Durability / Lifecycle	Cloud PCs are treated as dynamic, replaceable assets. (reprovisioning is acceptable)	Supports the "Cloud PC as a service" model and simplifies recovery from issues.	Reprovisioning results in a functional Day-One state without manual intervention.	Successful reprovisioning test; post-reprovision compliance + app install confirmation.
Storage Strategy	128 GB SSD is sufficient because primary data is stored in OneDrive/SharePoint.	Prevents local storage overuse and supports persistent cloud-first data governance.	Users store data in OneDrive/SharePoint, not local disk; disk usage remains under control.	Storage utilisation monitoring; KFM policy confirmation; user audits.
BYOD Device	Support an unmanaged version of Windows 11 that can log in to a cloud PC.	Makes the Cloud PC accessible for more use cases.	Company data is securely stored in the cloud and on the Cloud PC.	Users no longer use web access to Microsoft 365; they use Cloud PCs for productivity.

4.4.2. Windows 365 Provisioning

4.4.2.1. Background

Windows no longer uses a toolset for image design and configuration that focused on baking changes into a copy of the operating system called Microsoft Deployment Toolkit. That typically led to many applications being "baked" into the image by deploying the operating system on a virtual machine, installing software, and then sysprepping the machine to capture the disk contents.

For Windows 365, the provisioning policy sets key configurations, such as the network location and the image used. Being able to use networking and an image without your own configuration reduces friction during onboarding of Cloud PC technology and helps keep it current.



4.4.2.2. Decisions

Based on the information gathered, the design leverages several aspects of application deployment. A combination of image management and application deployment via Intune will be required to achieve the expected results and deliver the best user experience.

4.4.2.2.1. Windows 365 Image (Core Applications)

Because Microsoft 365 applications require significant installation time, it is recommended to use an image with the applications already installed. While this isn't the most highly customised Microsoft installation, it will be sufficient.

4.4.2.2.2. Network Location

Since the network must define the closest region for this test, the Geography is set to the US West region group.

4.4.2.2.3. Device Naming

Devices will start with the name "CPC-" to make them easier to group into a dynamic group. The rest of the device name will be a random combination of six numbers and letters.

4.4.2.2.4. Single Sign On

The default will be to enable single sign-on for Cloud PCs, as it is the most secure way to log in and re-evaluate compliance without excessive end-user prompting.

4.4.2.3. Decision Success Criteria

Decision Area	Decision	Success Criteria	How to Measure / Validate
Provisioning Model	Use Windows 365 provisioning policies with a mix of prebuilt	Cloud PCs are provisioned consistently with minimal manual intervention and a	Provision 5–10 Cloud PCs and confirm: • Successful provisioning rate ≥ 95%

	image + Intune app deployment.	predictable user experience.	• No manual rework required on baseline setup
Windows 365 Image (Core Apps)	Use an image with Microsoft 365 apps pre-installed.	Microsoft 365 apps are fully usable immediately after first login; they reduce first login/setup time.	Validate on first login: • MS 365 apps open without prompts/errors • Installation is not triggered post-provisioning • User can launch Word/Outlook within 2 minutes
Application Delivery via Intune	Deploy remaining apps via Intune.	Required apps install automatically within acceptable timeframes and reach expected compliance states.	Confirm with pilot users: • Apps install within defined SLA (e.g., 30–60 mins) • Intune shows ≥ 95% deployment success • No user escalation for missing apps
Network Location	Geography set to the US West region group.	Cloud PCs are created in the intended region, and the user experience (latency) is acceptable.	Confirm in the Windows 365 portal: • Cloud PC region = US West group • Average latency within acceptable threshold (e.g., < 80ms for test users) • No region mis-provisioning occurs
Device Naming	Prefix “CPC-” + random 6-character suffix.	Cloud PCs are easily identified and automatically grouped for policy targeting.	Validate naming standards: • All Cloud PCs are formatted as CPC-XXXXXX • Dynamic group membership includes 100% of Cloud PCs created under this policy
Dynamic Grouping (implicit)	Use a naming convention for dynamic grouping.	Devices automatically populate groups without manual assignment for policy deployment.	Validate: • New Cloud PCs appear in a dynamic group within 15–30 minutes • Configuration policies apply successfully to the group
Single Sign-On (SSO)	Enable SSO by default.	Users authenticate securely without excessive	Confirm pilot UX: • Users log in without repeated credential

		prompts, and compliance checks are enforced.	prompts • MFA/compliance behaviour matches policy expectations • Authentication errors < 5%
User Experience / Onboarding Friction	Reduce friction by using a standard image + Intune delivery.	Cloud PCs are ready to work quickly, and onboarding is smooth.	Measure: • Time from first sign-in to "ready-to-work" ≤ 15 minutes (core apps accessible) • Support tickets from onboarding ≤ defined threshold (e.g., < 1 per 10 users)

4.4.3. User Data

4.4.3.1. Overview

4.4.3.1.1. User settings

In a typical organisation, user settings are migrated between machines using a couple of technologies. OneDrive will remain the primary method for document and file storage, while Enterprise State Roaming will provide look-and-feel settings and modern application configurations. User Experience virtualisation still exists, but is no longer widely used.

Technology	In Use?
OneDrive Known Folders	Yes
Enterprise State Roaming	Yes
User Experience Virtualisation	No

4.4.3.2. Decisions

4.4.3.2.1. Use OneDrive and Enterprise State Roaming

Support data backups of frequently changing data. Also, the built-in snapshot capabilities in Windows 365 can roll back a Cloud PC's state in more extreme cases.

4.4.3.3. Decision Success Criteria

Decision Area	Decision / Standard	Why This Decision	Success Criteria	Validation / Evidence
Primary User Data Storage	User documents and files must be stored in OneDrive for Business using Known Folder Move (KFM).	Ensures user data persists independently of the Cloud PC lifecycle (reset/reprovision) and supports cloud-native data governance	Desktop, Documents, and Pictures folders automatically redirect to OneDrive for 100% of users.	OneDrive admin reports, client policy status, and user folder locations confirm the OneDrive path.

User Experience Settings	Enable Enterprise State Roaming (ESR) for profile-level cloud syncing.	Supports persistence of modern user settings such as themes, Edge settings, and app preferences across devices and re-provisioned Cloud PCs	Users retain key look-and-feel preferences after reconnecting or moving to a new Cloud PC.	ESR enabled tenant-wide; user test confirms settings persist after reprovision.
UE-V Usage	User Experience Virtualisation (UE-V) is not used.	UE-V is legacy and unnecessary when OneDrive + ESR meet the requirements; it reduces complexity and infra dependencies.	No reliance on UE-V tooling, GPOs, or file shares; experience persistence achieved through cloud services.	No UE-V configuration in environment; no UE-V agent required; settings persistence validated via ESR.
Cloud PC "Dynamic Asset" Model	Cloud PCs are treated as replaceable / reprovisionable assets, with settings/data externalised to cloud services.	Supports the "Cloud PC as a service" model — fixes become reprovisioning instead of complex remediation.	Reprovisioning results in a "day one" device that restores user experience quickly with minimal productivity impact.	The reprovision test confirms that OneDrive data and key user preferences have been restored.
User Communication & Training	Users receive guidance: save work to OneDrive. (not local disk)	Reduces risk of data loss during reprovisioning and reinforces cloud-first behaviour.	Users store work in OneDrive by default; low incidents of "lost files after reprovision".	Helpdesk ticket analysis; user survey results; OneDrive sync activity metrics.
Settings Persistence Scope	Focus persistence on M365 + Windows modern settings rather than full legacy roaming profiles.	Ensures predictable modern behaviour while avoiding bloated roaming profile dependencies.	Users retain M365 app preferences, Edge sync, and Windows settings across sessions without profile corruption.	ESR + Edge sync validated; user experience consistent after device refresh.
Recovery / Rollback Alignment	The profile strategy must support recovery tools, such as Windows 365	Ensures that in extreme cases, Cloud PC can be restored without	Restoring points does not cause permanent loss of user data due	Restore tests confirm user data remains accessible in

	restore points/snapshots.	compromising user-stored data.	to OneDrive backups.	OneDrive after rollback.
Support Model	Support teams must use “reprovision + OneDrive restore” as the preferred remediation path.	Reduces troubleshooting time and builds a scalable operational workflow.	IT can recover users quickly through reprovisioning rather than deep manual fixes.	Support runbook includes reprovision procedure; measurable reduction in time-to-recover.

4.5. System Management

4.5.1. Current State

Many enterprise environments have Intune; it is just a question of how extensively it is being used. It might not even be Windows management, so it isn't easy to make assumptions unless the environment is entirely new. Below is an example enterprise scenario with a history of Configuration Manager that may still be used for some devices.

Criteria	Value
Domain systems managed with?	Configuration Manager
Group Policy used?	Yes
Group Policy Preferences used?	Yes
Group Policy Security Baseline?	Yes, Microsoft
PowerShell currently used?	Yes
Systems are patched using (vendor, product & version)	Configuration Manager / WSUS
Mobile Device Management product	Intune

4.5.2. Decisions

For the Design, the following decisions were made to keep the design cloud native and optimised for Cloud PC.

4.5.2.1. **Discard any pre-existing group policy settings:** When deploying Cloud PCs on a Microsoft-hosted network with no domain services, it would likely be a waste of

time performing a detailed setting assessment and migration of settings. Use Microsoft Baselines and build from there.

4.5.2.2. **Do not migrate PowerShell scripts:** There is no need to migrate any technical debt. Keep the environment as clean as possible by not including old scripts into the Cloud PC environment.

4.5.2.3. **Use Security Baselines from Microsoft:** Intune has several baselines available for quick deployment to secure your devices and applications. To build the solution base, deploy the following baselines.

- Windows 365 Security Baseline
  - Applies strong default security controls to Cloud PCs (e.g., password policies, account lockout, firewall rules).
  - Helps prevent common cloud endpoint threats like credential theft, lateral movement, and weak device configurations.
- Microsoft 365 Apps for Enterprise Security Baseline
  - Reduces risk from malware and phishing by hardening Microsoft 365 application behaviour.
  - Helps control risky features like macros, add-ins, and ActiveX.
  - Enforces safer defaults for file handling and download protection.
- Security Baseline for Microsoft Edge
  - Enforces safe browsing protections (anti-phishing and anti-malware features).
  - Enables security features like SmartScreen, download restrictions, and secure browser configuration.
  - Controls how sites can access things like cookies, extensions, and scripting.

4.5.3. Decision Success Criteria

Decision Area	Decision / Standard	Why This Decision Matters	Success Criteria	Validation / Evidence
Legacy Configuration Approach	Discard any pre-existing Group Policy settings for Cloud PCs.	Cloud PCs are Entra Joined and built on a Microsoft-hosted network with no domain dependency, migrating GPOs adds effort with limited value and introduces policy complexity.	Cloud PCs deploy and operate successfully without reliance on Group Policy; baseline configuration is enforced through Intune only.	No Group Policy processing required; policy enforcement seen in Intune configuration status and device compliance.
Baseline Security Posture	Establish a clean baseline using Microsoft-recommended security controls	Reduces technical debt and ensures Cloud PCs start from a known, secure state	Devices meet security and compliance expectations without needing	Baseline reports show policies applied and compliant; no “gaps” requiring

	instead of legacy policy inheritance.	aligned with Microsoft cloud-first best practices.	legacy policy reconstruction.	GPO reintroduction.
Windows Hardening Baseline	Deploy the Windows 365 Security Baseline via Intune.	Ensures operating system settings are hardened specifically for the Windows 365 Cloud PC environment.	All Cloud PCs receive Windows 365 baseline settings and show successful policy deployment.	Intune baseline deployment status = successful; Endpoint Security reporting confirms baseline applied..
M365 App Hardening Baseline	Deploy the Microsoft 365 Apps for Enterprise Security Baseline.	Protects the primary productivity suite and reduces common attack vectors (macros, add-ins. legacy settings)	Microsoft 365 applications are hardened without negatively impacting normal user workflows.	Baseline assignment and compliance are visible in Intune; user validation confirms no major disruptions.
Browser Hardening Baseline	Deploy the Security Baseline for Microsoft Edge.	The browser is the most used app and most exposed to threats; hardening reduces phishing, extension risk, and unsafe browsing behaviour.	Edge is configured to a secure enterprise standard and remains consistent across Cloud PCs.	Edge baseline compliance reports; test shows policy enforcement. (extensions restricted SmartScreen enabled, etc.)
Policy Targeting Method	Apply baselines using dynamic Cloud PC device groups. (CPC-prefix)	Prevents manual targeting and ensures “zero-touch” security enforcement as new Cloud PCs are provisioned.	Newly provisioned Cloud PCs automatically receive baselines without intervention.	Dynamic group membership confirms inclusion; baseline assignment applies automatically on provisioning.
Operational Simplicity	Use Intune baselines and modern settings only. (Settings Catalog / Endpoint Security nodes)	Modern policy enforcement is easier to audit, more portable, and supports cloud operations without relying on line-of-sight DCs.	IT can manage and adjust baseline configuration entirely in Intune.	No GPO management required; configuration changes occur only through Intune, with change tracking.
Consistency & Drift Control	Use baseline deployment as the foundation and allow	Minimises drift and ensures support teams can trust a	Baselines stay consistent over time, and deviations are	Documented exception register; baseline

	deviations only by exception.	consistent Cloud PC posture.	documented and controlled.	comparison shows minimal drift.
Security Monitoring Readiness	Baseline deployment must be measurable and auditable in Intune reporting.	Ensures ongoing operational visibility and proves compliance to governance teams.	IT can produce baseline compliance reports at any time for the Cloud PC fleet.	Endpoint Security reporting, Intune compliance reporting, baseline comparison export.

4.6. Remote Access and System Protection

4.6.1. Current State

Providing secure access to the correct information is a key factor in improving employee productivity. The information and access methods must be adequately secured and comply with applicable compliance regulations.

Category	Manufacturer	Product Name	Usage
Antivirus	Microsoft	Windows Defender	Antivirus/Antimalware
Endpoint Detection and Response	N/A	N/A	N/A
VPN	N/A	N/A	N/A

4.6.2. Decisions

4.6.2.1. EDR is out of scope: This project will not cover EDR integration at this time, but it will be a broader consideration for the final project.

4.6.2.2. VPN is out of scope: VPN may be considered when not using custom networking with Windows 365, as a network path to Azure or on-premises resources may be required.

4.6.3. Decision Success Criteria

Decision Area	Decision / Standard	Why This Decision Matters	Success Criteria	Validation / Evidence
Endpoint Detection & Response (EDR)	EDR is out of scope for this pilot deployment.	Keeps the pilot focused on baseline Windows 365 enablement and avoids introducing additional licensing and operational complexity.	Cloud PCs are provisioned and operate securely without EDR agent dependency.	Intune app inventory shows no EDR agent installed; Windows Defender health status confirms AV running.

Security Baseline without EDR	Security posture relies on Windows 11 security features + Defender Antivirus + Intune baselines.	Since EDR is excluded, the environment must still meet a modern minimum security standard using built-in protections.	Defender Antivirus is active and healthy on 100% of Cloud PCs; security baselines are deployed and compliant.	Defender status reports; Intune Endpoint Security baseline reporting.
VPN Connectivity	VPN is out of scope for the pilot.	The deployment uses Microsoft-hosted networking and avoids on-prem connectivity dependency to maintain a clean cloud-first architecture.	Users access Cloud PCs successfully from the internet without VPN; no workflows require tunnel access.	Connection success tests from external networks; no VPN-related support incidents.
Resource Access Approach	Use cloud-native access paths (M365 / SaaS) rather than relying on on-prem resource connectivity.	Reinforces Zero Trust and reduces need for private routing or legacy dependencies.	Pilot users can perform required workflows through Microsoft 365 services without needing internal network access.	User validation; service access tests; workflow checklist confirms no blocked dependencies.
Conditional Access Enforcement	Windows 365 access is protected using Conditional Access policies.	With no VPN and no EDR, access control must still be strongly enforced at identity and session level.	CA policies apply to all Windows 365 sign-ins and enforce MFA and secure access requirements.	Entra sign-in logs show CA applied; test sign-ins confirm policy evaluation.
Future-State Security Roadmap	EDR and VPN are formally captured as future production considerations.	Ensures pilot exclusions don't become permanent gaps and supports production-ready security planning.	A documented roadmap exists for post-pilot enhancements. (EDR integration + networking strategy if needed)	Project backlog/roadmap references; architecture revision notes.

4.7. **Monitoring**

Effective management in a Zero Trust environment requires good visibility. Our monitoring approach relies on cloud-based services, such as Windows Telemetry and Azure Monitor, to collect device metrics. While these data sources cover the device, it is also essential to consider other relevant environmental sources, such as Entra and the Intune Service.

4.7.1. Entra ID

4.7.1.1. Current State

Entra ID currently exports no logs to Azure Monitor. All reporting is done using built-in features.

4.7.1.2. Decisions

4.7.1.2.1. Enable Entra ID Logging to Azure Monitor (Log Analytics)

This provides richer sign-in telemetry and additional Intune-related data for reporting.

Category	Success Criteria	Measurement / Validation
Log Enablement	Entra ID diagnostic logs are successfully streamed to Azure Monitor (Log Analytics).	Log Analytics workspace receives Entra sign-in and audit log records.
Log Coverage	Required log categories (Sign-in Logs and Audit Logs) are enabled.	Azure portal configuration confirms selected diagnostic log categories.
Data Continuity	Logs are ingested consistently, with no prolonged gaps during business hours.	KQL queries show continuous data within a rolling 24–72-hour window.
Sign-In Visibility	Administrators can query successful and failed sign-ins by user, application, and location.	KQL queries return to the expected fields (user, app, IP, location, result).
Correlation Capability	Entra sign-in data can be correlated with Intune or device context, where identifiers are available.	Queries demonstrate joins or filtered views using shared identifiers (e.g., user, device ID).
Security Monitoring	At least one alert is configured for suspicious sign-in activity.	The alert rule exists, is enabled, and triggers during controlled testing.
Operational Readiness	Alerts include documented ownership and response actions.	Runbook or operational documentation is available and reviewed.
Retention Management	Log retention is configured in accordance with organisational policy.	Log Analytics retention settings match defined requirements.
Cost Control	Log ingestion volume is monitored and is within expected cost thresholds.	Azure cost analysis shows predictable ingestion and budget alerts are configured.
Access Governance	Access to logs follows least-privilege RBAC principles.	Role assignments reviewed and approved by security/identity teams.
Maintainability	Logging configuration is documented and repeatable.	Documentation or IaC artefacts exist and are version-controlled.
Validation & Review	Periodic validation confirms logs and alerts remain functional.	The scheduled review confirms that data ingestion, alerts, and dashboards operate as expected.

4.7.2. Intune

Intune reporting uses a layered approach: it includes default functionality, but administrators can enable additional capabilities to provide deeper insights into the environment.

4.7.2.1. Current State

Currently, the environment uses the built-in reporting in Intune.

4.7.2.2. Decisions

4.7.2.2.1. Introduce Use of Cloud PC Reports

While no enablement is required, the following reports will be used to triage issues in the Cloud PC environment.

- Cloud PC Utilisation
- Cloud PC Recommendations
- Remoting Connection
- Resource Performance

4.7.2.2.2. Continue using existing Intune Reports

Many of the reports in the Intune console remain applicable to work with cloud PCs. Administrators can still view device compliance, patching, and device configuration details.

4.7.2.3. Decision Success Criteria

Decision	Objective	Success Criteria
Cloud PC Reports	Provide deep visibility into the performance and health of the Windows 365 fleet.	• Admins can identify under-utilised licenses via Cloud PC Utilisation reports. • Troubleshooting "poor connection" tickets is facilitated by Remoting Connection latency data. • Proactive right-sizing is performed using Resource Performance and Recommendations.
Intune Reports	Maintain a unified management "pane of glass" for both physical and virtual endpoints.	• Cloud PCs are 100% represented in Compliance and Configuration Profile status reports. • Windows Update reports accurately reflect patch levels across the Cloud PC environment. • Security posture remains consistent without requiring disparate tools.
Endpoint Analytics Integration	Measure the user experience (UX) impact of the Cloud PC transition.	• Startup Performance for Cloud PCs meets or exceeds the baseline of physical desktop performance. • Application Reliability reports show no significant increase in app crashes within the virtual environment.

4.7.3. Azure Monitor

4.7.3.1. Current State

Azure Monitor is not deployed for any of the workloads in scope. Entra, Intune and Windows are using built-in logging capabilities.

4.7.3.2. Decisions

4.7.3.2.1. Designate a Workspace

When building this solution, governance must account for the current Azure design and, where possible, follow best practices. The key concept is to place this workspace in a production subscription and have your Entra, Intune, and Windows 365 devices report to it.

4.7.3.2.2. Collect Entra ID Logs

Entra ID Sign-In logs will be sent to the same workspace as all other logging in the solution, supporting a centralised workspace for the core infrastructure.

4.7.3.2.3. Enable Intune Platform Logs

Enable this feature to help generate logs for auditing actions on the Intune platform. This supports change tracking and compliance by providing an audit trail for reference.

4.7.3.2.4. Enable Windows Update for Business Reports

Included with the Windows license, this feature enables the organisation to collect more in-depth data on Windows servicing across the fleet.

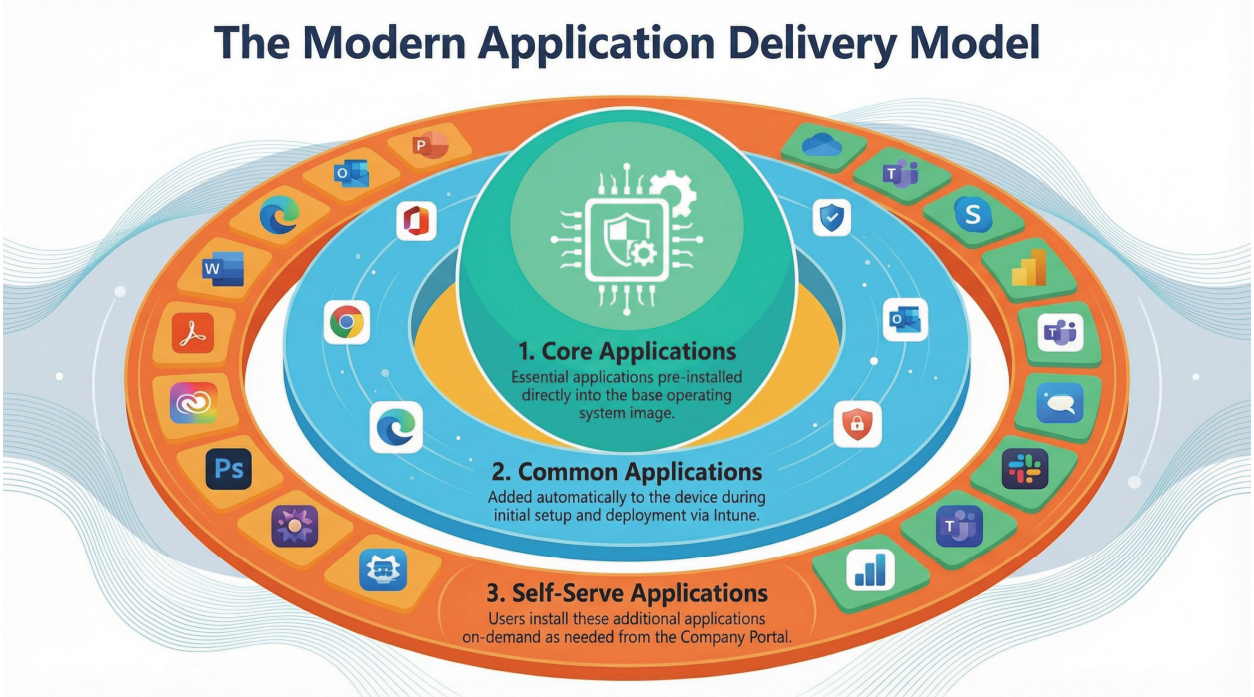
4.7.3.3. Decision Success Criteria

Decision	Objective	Success Criteria
Designate a Workspace	Establish a centralised logging and monitoring foundation for Windows 365, Intune, and Entra ID in alignment with governance and Azure best practices.	A Log Analytics workspace exists in a production subscription with defined ownership (Ops/Sec), RBAC, and naming standards. Data sources are connected (at minimum: Entra ID sign-in/audit logs, Intune platform logs once enabled, and Windows Update for Business Reports once enabled). A baseline retention policy is configured (e.g., 30 days) and validated against compliance requirements. Access is controlled via least privilege (e.g., Reader for support, Contributor for monitoring engineers, restricted admin access). A cost baseline is documented (expected daily ingest + retention impact) and monitored via Azure Cost Management.
Enable Intune Platform Logs	Provide auditability and change tracking for Intune administrative actions to support security operations,	Intune platform logging is enabled and actively ingesting into the designated workspace. Admin activity (policy create/update/delete, assignment changes, app deployment changes) is queryable in Log Analytics within an expected latency window

	compliance, and troubleshooting.	(e.g., < 15–60 minutes). At least three standard queries/workbooks exist and are validated by Ops/Sec (e.g., “Admin changes last 7 days”, “Changes by admin”, “High-risk configuration changes”). A repeatable investigation workflow exists for “what changed?” requests (e.g., identifying who changed a policy, when, and the scope of changes). Security/compliance stakeholders confirm that the logs are sufficient to meet audit trail requirements (or document any gaps and provide remediation actions).
Enable Windows Update for Business Reports	Improve depth and reliability of Windows servicing insights (compliance, failures, deployment progress) across the Cloud PC fleet for proactive operations and reporting.	Windows Update for Business Reports is enabled and ingests update telemetry into the workspace. Cloud PCs show high coverage in reporting (e.g., ≥95% of active Cloud PCs report within the last 7 days). Service dashboards/reports can answer questions such as patch compliance %, outstanding updates, error/failure codes, and deployment progress across rings/groups. Operations can identify and act on top failure patterns (e.g., top 5 error codes and affected devices) and track remediation outcomes over time. Patch reporting is consistent with Intune/Windows update views (differences are understood and documented), supporting a single operational narrative.

4.8. **Applications**

The user process for obtaining their applications is a three-phase journey. Many core applications are installed in the image, and additional typical applications are added during Intune device deployment. The user then uses the Company Portal to install any additional applications they need via self-service.



1. **Core Applications:** Limited to Windows 365. Custom images can expand options but also introduce complexity.
2. **Common Applications:** This software is usually delivered via Intune in a just-in-time fashion when the Cloud PC is built. Avoid user targeting.
3. **Self-Serve Applications:** Because Windows 365 users in this environment are not sharing machines, the option to make software available via the Company Portal application is recommended.

4.8.1. MSIX and UWP Applications

The richness and functionality of the applications influence users' productivity on Windows. Windows 11 offers a critical capability that enables developers and users to be productive on any Windows 11 device, while remaining secure and immersive.

4.8.1.1. Current State

The following information pertains to modern application formats on Windows and to applications on other platforms in a typical organisation’s desktop environment.

Currently using Modern applications?	Yes
Using MSIX?	Yes
Number of line-of-business modern apps	1-2

4.8.1.2. Decisions

Modern applications are not a high priority, but having a curated Company Portal is a starting point for the organisation. These applications are designed to be isolated by default, making them ideal for a self-service software deployment experience for the end user. The following activities will take place to establish a modern solution for Windows 11 Cloud PCs.

- Publish VLC Player (UWP) from the new store

The following applications will be delivered as part of the proof of concept.

- Company Portal - Required
- VLC Player (UWP) - Available

4.8.1.3. Design Success Criteria

Decision Area	Decision / Standard	Why This Decision Matters	Success Criteria	Validation / Evidence
Modern App Strategy	Modern applications are not a high priority for the pilot, but a curated Company Portal is established as a baseline capability.	Maintains focus on core provisioning outcomes while enabling future expansion into modern app delivery.	The pilot can function without heavy modern app dependencies, but modern app delivery is successfully validated.	Pilot users have full productivity baseline; Company Portal integration works for at least one validated app.
Modern App Delivery Platform	Modern apps are delivered using the Microsoft Company Portal integrated with Intune.	Eliminates repackaging and enables cloud-native app sourcing and lifecycle management.	Apps can be sourced, synchronised, and deployed without Win32 packaging.	Intune app list shows Store apps successfully imported/synced; deployment metrics show success.
Curated Company Portal Approach	Only approved modern apps are published — no open access to the consumer Store catalogue.	Reduces bloat, minimises attack surface, and prevents installation of unapproved consumer apps.	Users see only approved applications in the Company Portal; no uncontrolled Store access.	Company Portal library shows a curated list; Store access policies confirm restricted behaviour.
Reference Modern App	Publish the VLC Player (UWP) as a modern app for the proof of concept.	Serves as a low-risk test case to validate Store → Intune → Company Portal.	VLC appears in the Company Portal and installs successfully when requested.	Company Portal shows VLC as Available; installation completes successfully on multiple Cloud PCs.

		deployment workflow		
App Availability Model	VLC is deployed as Available (self-service), not Required.	Prevents unnecessary application bloat while validating self-service workflows.	Users can install VLC when needed; devices are not forced to install it.	Intune assignment confirms “Available for enrolled devices”; user validation confirms install is optional.
User Empowerment Model	Self-service installs are enabled using Company Portal.	Reduces helpdesk workload and supports lightweight persona variability.	Users can install optional apps without admin intervention and without local admin rights.	User test confirms install without admin prompts; helpdesk ticket volume reduced for software requests.
Security Posture of Modern Apps	Modern apps are accepted because they are isolated by default and aligned with enterprise app governance.	Supports secure and controlled software expansion without legacy installer risk.	Modern apps deploy without requiring elevated privileges or risky install scripts.	Successful deployment metrics; no security exception required for app install.
Operational Readiness	Modern app publishing must be repeatable and manageable through Intune.	Ensures the pilot delivery method becomes a scalable operational model.	IT can add another Store app using the same workflow without redesign.	Admin runbook validated; repeatable deployment workflow test completed.

4.8.2. Win32 Applications

4.8.2.1. Current State

For years, desktop applications (often referred to as “Win32 apps”) have made up most of the enterprise application portfolio and typically include critical, line-of-business applications.

4.8.2.2. Decisions

The following line of business Win32 applications will be included with every deployed Windows device:

- 7-Zip (repackage)
- Microsoft 365 (in image)
- Remote Help

As part of the design, the 7-Zip and Remote Help packages must be built and tested with Intune before creating the first pilot Cloud PCs. Microsoft 365 is listed in the gallery image for the Operating System, so packaging it is not required.

4.8.2.3. Decision Success Criteria

Decision Area	Decision / Standard	Why This Decision Matters	Success Criteria	Validation / Evidence
Win32 Delivery Platform	All Win32 apps will be delivered via Microsoft Intune using the Intune Management Extension (IME).	Ensures the deployment model aligns with Cloud PC management and avoids dependence on legacy tooling. (SCCM/GPO)	Required Win32 apps install automatically on provisioned Cloud PCs without manual admin intervention.	Intune app deployment status = Installed; IME logs confirm execution; Apps visible in Settings/Control Panel or inventory.
Packaging Standard	Win32 apps must be packaged as .intunewin with silent install commands, uninstall commands, and reliable detection rules.	Ensures predictable installations and avoids “false success” reporting, partial installs, or user prompts.	100% of baseline Win32 apps install silently, and detection rules accurately confirm install/uninstall state.	Install/uninstall tests on pilot ring devices; detection outcomes in Intune; IME logs; no user prompts observed.
Baseline Win32 Applications	Baseline Win32 apps included on every Cloud PC: 7-Zip (repackage) and Remote Help. Microsoft 365 is included via a gallery image.	Guarantees core baseline utilities and support tooling exist on every device; aligns with operational needs.	Every Cloud PC has 7-Zip + Remote Help installed and functional post-provisioning.	Intune Required app deployment reports; spot checks in pilot ring; functional confirmation (launch + version check).
Microsoft 365 Delivery Method	Microsoft 365 is delivered through the Windows gallery image (not packaged separately).	Prevents redundancy, reduces provisioning time, and avoids version mismatch or additional deployment complexity.	Microsoft 365 apps are available immediately after provisioning and comply with organisational licensing/config policies.	Cloud PC image configuration validation; Microsoft 365 apps present; licensing activated; baseline user test confirms functionality.
Testing Requirement (Pre-Pilot)	7-Zip and Remote Help packages must be built and validated in Intune before enabling provisioning policies for pilot users.	Packaging failures are a high-risk issue in provisioning; early testing reduces pilot disruption and support load.	Baseline app packages are validated in a test ring with no critical install failures before pilot creation.	Test ring deployment success ≥ 95% (or agreed threshold); IME logs reviewed; provisioning results show no app-related failures.

Scope Control	Only critical baseline Win32 apps are included initially; additional Win32 apps are introduced incrementally based on pilot needs.	Avoids baseline creep, long provisioning times, and troubleshooting overload during early rollout.	Pilot Cloud PCs meet productivity + support requirements with minimal provisioning delays and stable baselines.	Provisioning time metrics stay within target; failure rates are low; pilot feedback shows baseline sufficient.
Operational Supportability	Win32 app deployment must be supportable via Intune reporting, logs, and remediation workflows.	Failures will occur; IT must quickly diagnose and remediate without rebuilding devices.	Win32 deployment failures are detectable, diagnosable, and remediable within a defined SLA (ex, < 1 business day).	Intune reporting dashboards; IME logs; known troubleshooting steps/runbooks; remediation scripts available.
Update Strategy for Win32 Apps	Win32 apps must be maintained via Intune version control using a Supersedence or replacement strategy.	Prevents version drift and ensures security updates are applied consistently across Cloud PCs.	Most Cloud PCs run the approved versions; outdated versions are reduced and corrected.	Intune app version reporting; superseded policies verified; compliance baseline or reporting confirms version adherence.
User Privilege Alignment	Win32 apps must install successfully without requiring local admin rights.	Supports the least privilege model and avoids pilot failures caused by UAC prompts or admin dependencies.	Baseline apps installs when the device is provisioned.	Application installation via Intune requires no elevation of the user.

4.8.3. Browser Applications

Modern Application Architecture
The core value of web applications lies in decoupling the application from the underlying hardware. By centralising code on a web server, organisations achieve "Write Once, Run Anywhere" (WORA) efficiency.

Zero-Footprint Deployment: Unlike traditional Win32 or macOS apps, web apps require no local installation, registry modifications, or complex uninstallation routines. This reduces "software rot" on the endpoint.

On-Demand Delivery: Modern web apps use Single-Page Application (SPA) frameworks (such as React or Angular). Instead of refreshing the whole page, they dynamically update content, making the web experience feel as fluid as a local desktop application.

The Rise of PWAs: Progressive Web Apps have further bridged the gap, enabling web apps to work offline, send push notifications, and sit in the taskbar while still being served from a central web URL.

Where developers spent 40% of their time fixing CSS for Internet Explorer has shifted mainly due to two major industry movements:

The Chromium Hegemony: Most modern browsers (Microsoft Edge, Google Chrome, Brave, Opera) are now built on the Chromium engine. This has standardised rendering behaviours, drastically reducing the effort needed for "cross-browser" tweaking.

Modern Web Standards: The maturation of HTML5, CSS3, and WebAssembly (Wasm) has provided a robust, high-performance toolkit that works consistently across devices, including mobile and tablets.

However, the challenge has pivoted from visual consistency to performance optimisation and managing the massive memory footprint that modern browsers require.

The browser's success is its greatest vulnerability. In many modern "Cloud-First" organisations, the browser is effectively the Operating System. If a hacker controls the browser, they control the keys to the kingdom.

Modern Security Threats
While the 2017 perspective focused on "gaining access to workstations," the threat in 2025 is often more focused on Identity and Data Exfiltration:

- **Session and Token Theft:** Instead of installing a virus, attackers now use "Adversary-in-the-Middle" (AiTM) attacks to steal session cookies. This allows them to bypass Multi-Factor Authentication (MFA) and directly impersonate the user in cloud apps such as Microsoft 365 or Salesforce.

- **Malicious Extensions:** Browser extensions have become a "blind spot" for IT. A seemingly helpful PDF converter might be a keylogger or a data scraper operating within the browser's memory.

- **Browser-in-the-Browser (BitB) Attacks:** Attackers create fake browser windows within a legitimate web page to trick users into entering credentials, making phishing nearly indistinguishable from a legitimate login prompt.

- **Hardening The Portal:** Because organisations can no longer rely solely on traditional antivirus software to protect a web session, they have adopted new defensive layers:

- **Enterprise Managed Browsers:** Companies now use policies to "lock down" the browser (e.g., disabling unsanctioned extensions, forcing password synchronisation, and isolating personal vs. work data).

- **Remote Browser Isolation (RBI):** High-risk web traffic is executed in a disposable container in the cloud. Only a visual stream of the website is sent to the user’s device, ensuring that if a site is malicious, the code never touches the local workstation.

- **Zero Trust Access:** Moving away from VPNs toward ZTNA (Zero Trust Network Access), where the browser must prove the user's identity and the device's health before the web application will even "acknowledge" the connection.

Key Takeaway: The web browser is no longer just a document viewer; it is the most critical enterprise application in the stack. Consequently, browser security is no longer an "IT task"; it is a core pillar of cybersecurity strategy.

4.8.3.1. Current State

In this architecture, the following is a typical scenario for browsers. There are often "supported" browsers, but inventory data on machines usually tells a different story.

Primary desktop browser and version	Edge Chromium
Other browsers used in the organisation	Edge, Google Chrome, Mozilla Firefox
Using Internet Explorer 11	No

4.8.3.2. Decisions

Based on the inventory data and the organisational goal of streamlining endpoint management, the following architectural decisions have been made:

4.8.3.2.1. Standardise on Microsoft Edge (Chromium)

- **Decision:** Microsoft Edge will be the primary, supported enterprise browser for all managed devices.
- **Justification:** Edge Chromium provides the highest level of integration with Microsoft 365 security services, including Microsoft Defender SmartScreen and Conditional Access policies. It enables a single sign-on (SSO) experience with Entra ID (Azure AD) and synchronises user settings across the Windows 365 environment.
- **Security Alignment:** By standardising on Edge, the organisation can utilise Microsoft Endpoint Manager (Intune) to enforce security baselines, such as disabling unauthorised extensions and enforcing "Strict" tracking

4.8.3.2.2. Formalise "Secondary" Browser Support & Containment

- **Decision:** Google Chrome and Mozilla Firefox will be moved to a "Legacy/Restricted" support tier.
- **Implementation:** No alternate browsers will be offered in the Company Portal.
- **Mozilla Firefox:** To be phased out unless a specific business justification (e.g., a particular development or testing requirement) is provided.
- **Rationale:** Reducing the number of installed browsers minimises the attack surface and reduces the "DLL sprawl" often associated with multiple rendering engines.

4.8.3.2.3. Address Legacy Compatibility (IE Mode)

- **Decision:** While Internet Explorer 11 is not used as a standalone browser, it is prudent to disable this feature unless needed.

- **Goal:** If inventory data or user experience later reveals legacy apps that require IE engines, they will be rendered inside Edge using IE Mode. This ensures the IE11 application remains disabled at the OS level while maintaining backward compatibility.

4.8.3.3. Decision Success Criteria

Decision Area	Decision / Standard	Why This Decision Matters	Success Criteria	Validation / Evidence
Secondary Browser Strategy	Google Chrome and Mozilla Firefox are classified as Legacy / Restricted browsers.	Reduces attack surface, limits browser sprawl, and enforces a predictable supported baseline for security + troubleshooting.	Only Edge is supported as the primary browser; Chrome/Firefox usage is minimal or nonexistent.	Software inventory shows Edge as dominant; usage telemetry confirms little to no Chrome/Firefox adoption.
Software Availability Model	No alternate browsers will be offered in the Company Portal.	Prevents users from installing unnecessary browsers and avoids unmanaged extension ecosystems.	Company Portal does not provide Chrome or Firefox; Edge remains the only browser delivered and maintained.	Company Portal app catalogue confirms browsers not available; app assignment settings verify exclusions.
Mozilla Firefox Lifecycle	Mozilla Firefox is to be phased out, unless a formal business exception is approved.	Firefox introduces a separate rendering/security model, requiring additional policy management and operational support.	Firefox is removed or absent from Cloud PCs unless explicitly justified; exceptions are rare and documented.	App inventory confirms removal/absence; exception register exists for approved business cases.
Exception Handling Process	Alternate browsers require a documented business justification and a controlled deployment method.	Ensures browser diversity is limited to only cases where it is genuinely required for workflow continuity.	Any alternate browser present is traceable to an approved exception and targeted deployment.	Exception request log; Intune assignment scope proves controlled targeting.
Security and Compliance	Reducing browser count minimises extension-based risk, token theft exposure, and overall web attack surface.	Multiple browsers increase security drift (extensions, updates, policies). A single-browser strategy makes hardening enforceable.	The environment maintains a consistent browser security posture through Edge baseline and policy enforcement.	Edge security baseline compliance; extension control enforcement evidence.

Support and Operations	Support model is simplified to "Edge-first" troubleshooting.	Helpdesk troubleshooting becomes consistent; reduces "works in browser X but not Y" complexity.	Reduced browser-related tickets and faster incident resolution due to standardisation.	Ticket trend analysis: reduced browser compatibility troubleshooting time.
Update & Servicing Consistency	Browser servicing and version control are simplified by standardising on Edge only.	Ensures update cadence, patch compliance, and reduces the risk of outdated browsers in the fleet.	All Cloud PCs remain within acceptable Edge version compliance and do not require Chrome/Firefox patching workflows.	Edge version reporting and servicing dashboards. (Autopatch or Intune reporting)

4.8.4. Microsoft 365

4.8.4.1. Current State

Most organisations use Microsoft 365 for most users because it leverages and integrates most closely with Microsoft 365 cloud services. Knowledge workers typically rely on one or more Microsoft 365 applications for day-to-day work.

Microsoft 365 Suites Currently in use	Microsoft 365
Number of Language Packs required	0
Preferred installation method (MSI vs. C2R)	C2R
Preferred activation technology	Cloud
Would Office be included with the Windows 10 reference image?	No
Microsoft 365 is configured via GPO?	Yes
Is Microsoft 365 configured via MDM?	Np
Is Microsoft 365 configured via Office Cloud Policies	No

4.8.4.2. Decisions

4.8.4.2.1. Detailed Servicing Decisions

The following table summarises the core components of the M365 servicing model:

Component	Decision	Rationale
Delivery Mechanism	Part of image.	Standardises the application environment and ensures seamless integration with Windows 365 provisioning.
Update Management	Windows Autopatch	Shifts the burden of update orchestration, ring management, and monitoring to Microsoft's automated service.

Security Configuration	Intune Security Baselines	Implements a Microsoft-recommended set of best practices for M365 hardening to ensure a known-secure state.

4.8.4.2.2. Deployment & Configuration Details

Microsoft 365 Delivery via Cloud PC Image
To ensure a consistent user experience, Microsoft 365 Apps for Enterprise will be delivered as part of the Windows 365 (Cloud PC) provisioning process.

- **Standardisation:** Using the built-in Cloud PC image ensures that M365 apps are pre-optimised for virtual environments, including specific configurations for Outlook and Teams (e.g., media optimisations).

- **Provisioning Speed:** New users receive a fully functional productivity suite immediately upon the creation of their Cloud PC, eliminating the wait time associated with post-deployment application installs.

Automated Servicing with Windows Autopatch
The organisation will utilise Windows Autopatch to manage the lifecycle of M365 updates. This decision moves away from manual "Update Ring" management in favour of an AI-driven approach.

- **Progressive Deployment:** Autopatch automatically assigns devices into Test, Fast, and Broad rings, ensuring that a subset of users validates updates before reaching the entire environment.

- **Conflict Resolution:** Autopatch monitors for update failures or performance regressions; if a significant issue is detected, the service can automatically pause or roll back updates to prevent widespread downtime.

- **Reporting:** Real-time dashboards within the Microsoft Intune admin centre will be used to track update compliance and health status.

Security Hardening via Intune Baselines
The Microsoft 365 Security Baseline will govern security for the M365 suite for Intune.

- **Best-Practice Alignment:** By adopting the baseline, the organisation adheres to Microsoft's recommended security posture, which includes hardened settings for macro execution, add-in management, and credential protection.

- **Simplified Auditing:** Using a standard baseline makes it easier to identify configuration drift. Any deviations from the baseline can be quickly identified and remediated through the Endpoint Security node in Intune.

- **Minimal Friction:** The baseline is designed to maximise security without disrupting common productivity workflows, striking an optimal balance for the end-user.

4.8.4.3. Decision Success Criteria

Decision Area	Decision / Standard	Why This Decision Matters	Success Criteria	Validation / Evidence
M365 App Standard	All Cloud PCs will use Microsoft 365 Apps for Enterprise. (Click-to-Run)	Provides a supported evergreen productivity suite, aligns with the licensing model, and avoids legacy MSI deployment.	100% of Cloud PCs have Microsoft 365 Apps installed and functional.	App inventory confirms install; user validation confirms apps launch + activate.
Inclusion Method	Microsoft 365 Apps are included via the Windows 11 Gallery Image. (not manually installed post-provision)	Reduces provisioning complexity and ensures a predictable Day-One experience.	Cloud PCs provisioned with M365 Apps are available on first login.	Provisioning validation confirms apps are present immediately after creation.
Configuration Authority	Microsoft 365 Apps are configured and secured via Intune policy. (Settings Catalogue + security baselines)	Ensures centralised control of update channels, macro settings, and security posture and prevents drift.	M365 Apps baseline policies apply successfully and align with security posture goals.	Intune policy deployment reports; baseline compliance reporting.
Update Channel Strategy	Office update channel follows Microsoft-recommended enterprise servicing. (e.g., Monthly Enterprise Channel)	Provides a predictable cadence with security patches and reduces disruption risk.	Devices stay within the acceptable patch compliance window and update without user disruption.	Update compliance reports; Office version reporting; pilot user feedback.
Licensing Activation Model	M365 apps activate via user sign-in. (Entra ID / M365 licensing)	Ensures seamless activation and avoids shared-key / manual activation complexity.	Users experience automatic activation without prompts or licensing failures.	User validation, activation status in Office account settings, and sign-in logs.

App Consistency & Standardisation	Only the supported M365 Apps suite is used. (No Office perpetual editions in pilot)	Prevents version fragmentation and reduces support complexity.	No Cloud PCs contain legacy Office versions; support is standardised.	Software inventory confirms no MSI/perpetual Office versions installed.
Security & Compliance Controls	Office security posture is hardened using the M365 application security baseline.	Office is a common attack vector (macros, phishing, add-ins); baseline controls reduce risk.	Macro settings, Protected View, and security controls enforce the expected baseline behaviour	Baseline compliance reports; macro testing confirms expected restrictions.
User Readiness & Supportability	Users can access OneDrive, Teams, Outlook, and Office apps on Day One without additional installs.	Enables productivity immediately and reduces support tickets in the early pilot stage.	Pilot users can complete core workflows (Teams calls, Outlook, Word/Excel collaboration) on Day One.	Pilot validation checklist; user survey results; reduced “missing apps” tickets.
Integration with Cloud Storage	Office apps are aligned to OneDrive/SharePoint for storage by default.	Supports a cloud-first storage strategy and reduces data loss risk on reprovision.	Users save/auto-save to OneDrive/SharePoint by default.	OneDrive sync status, known folder move config, and user storage behaviour confirmation.

4.9. Look and Feel

4.9.1. Current State

A custom taskbar that has Outlook pinned is present on physical devices. The Start menu in Windows 11 is positioned in the left corner of the screen.

4.9.2. Decisions

4.9.2.1.1. Use the Default Layout

To reduce customisation and maintenance, the default Windows 365 layout from the image will be used.

4.9.2.1.2. Unpin Microsoft Store from Taskbar

Use Default Start/Taskbar Layout. To minimise customisation and maintenance, we will retain the default layout provided by the base Windows 365 image (no custom taskbar or Start menu configuration).

4.9.3. Decision Success Criteria

Decision	What we're changing	Success criteria	How to validate
Use the Default Layout	Cloud PCs will use the default Windows 365 image layout (no custom taskbar/start layout). Physical devices currently have a custom taskbar (Outlook pinned) and a Windows 11 Start aligned to the left.	1) No custom Start/Taskbar layout policy is applied to Cloud PCs. 2) Newly provisioned Cloud PCs show the default taskbar and Start menu configuration for the base image. 3) No service requests are raised for missing pinned apps that were previously 'standard' within the first 30 days of rollout.	Intune: Confirm that no device configuration profile is enforcing Start/Taskbar layout for the Cloud PC group(s). Spot-check: provision 3–5 new Cloud PCs and visually confirm the default layout. Helpdesk trend: review tickets tagged "taskbar/start" after rollout.
Unpin Windows Store from Taskbar	Microsoft Store will still exist (as required for app servicing), but it will be unpinned from the taskbar to reduce clutter.	1) On Cloud PCs, the Microsoft Store is not pinned to the taskbar for new deployments. 2) Store still functions in the background for modern app servicing (no increase in Store/framework update failures). 3) No user impact to required apps/components that rely on Store servicing (e.g., framework updates).	Spot-check: provision 3–5 Cloud PCs and confirm the Store icon is not pinned. Validate servicing health: monitor Store/app update status (Intune app update signals/event logs if you're collecting). Support: confirm no spike in tickets for Store-dependent apps.

4.10. Clipboard File and Print

4.10.1. Current State

There is currently no AVD environment to reference for baseline settings for these behaviours.

4.10.2. Decisions

4.10.2.1. Enable Clipboard Redirection

This is a low-risk change that improves user productivity by allowing copy-paste between the local device and the Cloud PC. *(Microsoft's default is to block clipboard redirection for security, but that default can hinder day-to-day tasks.)*

4.10.2.2. Disable Printer Redirection

Cloud PCs will not redirect print jobs to local printers. (Any required printing would need to use a cloud-print service, which is outside the scope of this pilot; printing will only be enabled as an exception if absolutely needed.

4.10.2.3. Block File Redirection

If users need to transfer files, they must use approved methods like OneDrive or email (no direct drive mapping).

4.10.3. Decision Success Criteria

Decision	Rationale	Configuration / Control	Success criteria
Allow Clipboard	Improves day-to-day usability and productivity; considered low risk compared to file/printer redirection.	Enable clipboard redirection between the local endpoint and Cloud PC (Windows 365 policy / Cloud PC connectivity settings).	1) Users can copy/paste text between local and Cloud PC reliably. 2) No widespread helpdesk incidents related to the clipboard being blocked. 3) No security incidents attributed to clipboard usage beyond accepted risk.
Block Printer Redirection	Reduces data leakage paths and unmanaged print sprawl; printing is handled through controlled cloud print as an exception only.	Disable printer redirection from endpoint to Cloud PC (Windows 365 / RDP redirection controls).	By default, no Cloud PCs will have local printers mapped. Printing will be done as an exception to the design.
Block File Redirection	Prevents common malware ingress and reduces data exfiltration via mapped drives / redirected storage.	Disable file/drive redirection (local drives, removable media, file transfer paths) between the endpoint and Cloud PC.	1) Local drives/removable storage do not appear in the Cloud PC session. 2) Users cannot transfer files via redirection mechanisms (drag/drop / mapped local drives). 3) File movement occurs only via approved channels (OneDrive/SharePoint/Outlook) and is auditable.

4.11. Servicing

4.11.1. Windows as a Service

Microsoft delivers Windows 11 feature enhancements through a continuous servicing model commonly referred to as Windows as a Service. Under this model, new functionality is introduced through annual feature updates, released to the Windows 11 General Availability (GA) Channel.

The GA Channel represents the primary production release of Windows 11 feature updates and is the recommended servicing channel for most organisational devices. Legacy servicing terms such as Current

Branch and Current Branch for Business are no longer applicable and are not used in Windows 11 servicing. All devices receive feature updates from the same GA Channel release, with deployment timing controlled through update management policies rather than separate channels.

Each Windows 11 GA Channel release is supported for 24 months for Enterprise and Education editions. During this servicing window, organisations are expected to plan, test, and complete upgrades to the next GA Channel release. As a result, multiple supported Windows 11 GA Channel versions may coexist in the environment.

The initial GA Channel release of a Windows 11 feature update is used as the baseline for feature evaluation, pilot deployments, and validation of business-critical applications. This approach enables organisations to assess new capabilities early while managing risk through phased deployment strategies.

4.11.1.1. Current State

The current desktop estate will serve as a reference, though Cloud PCs must follow Microsoft's cadence for the best experience.

Current Versions of Windows Deployed	24H2
Current Servicing Technology	WUfB / Intune

4.11.1.2. Decisions

The following architectural decisions have been made to ensure the Windows 365 environment remains secure, performant, and aligned with Microsoft's long-term servicing roadmap.

4.11.1.2.1. Standardisation on Windows 11 25H2

It has been decided to standardise all Cloud PCs on Windows 11 version 25H2. This version represents the latest feature update, providing the most extended support lifecycle and access to the most recent productivity enhancements.

Justification:

- **Lifecycle Longevity:** By starting on 25H2, the organisation maximises the 36-month support window (for Enterprise editions), reducing the frequency of required "in-place" version upgrades.
- **Performance Optimisation:** Windows 11 is optimised explicitly for virtualised environments, offering improved resource scheduling and lower latency for Windows 365 sessions compared to older builds.
- **Security Baseline:** 25H2 includes the most current hardware-backed security features (TPM 2.0, Secure Boot, and VBS) enabled by default, which are critical for protecting data in a cloud-hosted environment.
- **Impact:** All custom images or gallery-based provisioning policies will be locked to this version to ensure environment parity and simplified troubleshooting.

4.11.1.2.2. Implementation of Windows Autopatch

To manage the ongoing servicing of the OS and Microsoft 365 Apps, the organisation will utilise Windows Autopatch rather than traditional manual rings in Intune. Windows Autopatch (built

on Windows Update for Business) automates the entire update ring orchestration. It manages deployments, monitors Cloud PC health, and can pause updates automatically if issues are detected, thereby removing the traditional manual burden from IT.

Justification:

- **Reduced Administrative Overhead:** Autopatch automates the creation of update rings (Test, Fast, First, and Broad), removing the need for manual configuration and monitoring by IT staff.
- **Reliability through Progressive Deployment:** Autopatch uses signals from the global Microsoft ecosystem to pause updates automatically if issues are detected, significantly reducing the risk of "patch Tuesday" regressions impacting productivity.
- **Reporting and Compliance:** It provides a consolidated dashboard for updated health, offering higher visibility into the patch status of the Windows 365 fleet compared to standard Windows Update for Business (WUfB) reports.
- **Impact:** Cloud PCs will be automatically enrolled in the Autopatch service upon provisioning. This requires that the Intune environment meet the specific prerequisite settings for "Health Monitoring" and "Data Collection".

4.11.1.2.3. Service Channel Alignment

The environment will align with the General Availability (GA) Channel (formerly Semi-Annual Channel) to balance stability and innovation.

- **Justification:** This ensures that the Windows 365 fleet stays on a production-ready path, avoiding the potential instability of Insider or Preview builds while still receiving annual feature updates that keep the environment modern.
- **Impact:** Policies will be configured to prevent Cloud PCs from drifting into the Windows Insider Program unless specifically designated for a "Pilot" group.

4.11.1.3. Decision Success Criteria

Decision / Standard	Why This Decision Matters	Success Criteria	Validation / Evidence
Standardise all Cloud PCs on Windows 11 Enterprise 25H2	Maximises support lifecycle, improves performance in virtualised environments, and ensures the latest security baseline is in place.	100% of Cloud PCs report OS version = 25H2 (no drift). New provisioning policies are pinned/locked to 25H2.	Intune device inventory (OS version), Windows 365 portal device details, provisioning policy configuration review.
Use Windows Autopatch (built on Windows Update for Business) as the primary servicing	Reduces manual ring management by automating deployments, monitoring device health, and pausing	All Cloud PCs are enrolled in Autopatch and assigned to update rings. OS quality updates deploy successfully with no widespread regressions; health	Windows Autopatch dashboard (enrollment, ring assignment, update status), Intune update reports,

method for Cloud PCs	updates when issues are detected.	dashboards remain 'Healthy'.	incident/rollback logs if applicable.
Enable required tenant prerequisites (Health Monitoring + Data Collection) to support Autopatch enrollment.	Autopatch enrollment and reporting depend on required telemetry/health monitoring settings.	Tenant prerequisites are enabled and validated; Cloud PCs enrol in Autopatch without prerequisite errors.	Autopatch setup checklist completed; Intune tenant settings confirm Health Monitoring + Data Collection; Autopatch enrollment success.
Define Autopatch compliance SLAs for Cloud PCs (Quality + Feature updates)	Makes servicing measurable, enforceable, and auditable; aligns IT ops expectations with user impact and security posture.	Monthly quality updates reach ≥95% compliance within 7 days of release. Feature updates reach ≥90% compliance within 60 days of rollout start. Devices that do not meet the SLA are flagged and remediated within 5 business days.	Autopatch compliance reports, Intune Update Compliance reports, the monthly patch KPI dashboard, and remediation tickets.
Establish an Autopatch exception process (documented business justification + expiry)	Prevents "permanent exemptions" that silently create security risk and unmanaged drift; supports audit readiness.	All patch deferrals/exceptions require documented justification, approver, and expiry date. Exception review occurs monthly; expired exceptions are removed or re-approved. Exception population remains <5% of fleet.	Exception register (SharePoint/CMDB), change records, Autopatch/Intune policy audit, and monthly exception review logs.
Define "widespread regression" thresholds and Autopatch pause/runbook criteria.	Ensures rapid, consistent responses when updates cause issues; avoids prolonged outages and ad hoc decision-making.	Regression threshold defined (e.g., >2% failure rate or any P1 incident). Autopatch pause is initiated within 24 hours when the threshold is met. Root cause analysis completed within five business days, and resolution action documented.	Autopatch pause/hold events, service desk incident logs, rollback logs, and post-incident review documentation.
Implement a monthly servicing governance cadence (Patch Health Review)	Creates an operating rhythm for servicing performance, risk, and continuous improvement; ensures compliance doesn't drift.	Monthly review occurs with an agreed agenda: compliance %, failure rate, exceptions, user impact, and upcoming feature updates. Action items recorded and closed within agreed timeframes.	Meeting minutes, compliance dashboards, action log, change calendar, governance deck/report.

Enable reporting and alerting for update compliance breaches	Ensure SLA violations are visible and acted upon rather than discovered during audits or incidents.	Automated alert triggered when quality update compliance drops below SLA (e.g., <95% within 7 days). Non-compliant devices generate remediation tasks within two business days.	Intune report exports, Autopatch reporting, alert rules/configuration, service desk tickets, remediation logs/scripts.
Require a documented validation window for the Autopatch Test ring before broad rollout	Increases confidence before broad rollout; provides a precise "go/no-go" mechanism and reduces impact of regressions.	Test ring receives updates first; validation is completed within 3–5 business days of release. The go/no-go decision is documented; issues result in a pause/hold before reaching the broad rings.	Autopatch ring membership, validation checklist, change record, pause/hold history, release notes & sign-off evidence.

4.11.2. Microsoft 365 as a Service

The delivery and servicing of Microsoft 365 Apps (formerly Office 365) within the Windows 365 environment are designed to balance user productivity with enterprise-grade stability. By treating Microsoft 365 as a continuous service rather than a static product, the organisation ensures that Cloud PC users always have access to the latest feature sets and security mitigations.

4.11.2.1. Current State

Historically, the Microsoft 365 install base has been fragmented across different update cadences:

- **Semi-Annual Enterprise Channel:** Most of the current install base resides here, receiving feature updates only twice a year. While stable, this often results in a "feature gap" where Cloud PC users lack the latest collaborative tools available in web-based versions of the suite.
- **Monthly Enterprise Channel:** A subset of users is on this channel, receiving updates once a month on a predictable schedule.
- **Management Overhead:** Current update cycles require manual intervention and validation, leading to version drift across the environment.

4.11.2.2. Decisions

To modernise the Microsoft 365 implementation on Windows 365, the following architectural decisions have been made.

4.11.2.2.1. Intune-Driven Management

All Microsoft 365 App deployments and configurations will be managed exclusively via Microsoft Intune. This centralises the policy set, ensuring that "Microsoft 365" settings (such as macro behaviours and security baselines) are applied consistently across all Cloud PC provisioning policies.

4.11.2.2.2. Standardising on the "Current Channel"

The organisation will transition end users to the Current Channel.

Justification: Windows 365 users benefit most from high-cadence updates that align with the rapid evolution of Microsoft 365 cloud services (e.g., Copilot integrations, Teams enhancements).

User Experience: This ensures users can access new features as soon as they are generally available, maintaining parity with the "evergreen" nature of the Cloud PC platform.

4.11.2.2.3. Automated Servicing via Windows Autopatch

Windows Autopatch will replace the manual overhead of managing Microsoft 365 update rings. Microsoft 365 patching will be enabled.

Progressive Deployment: Autopatch will automatically categorise Cloud PCs into "Test," "First," "Fast," and "Broad" rings.

Health Monitoring: If a Microsoft 365 App update causes performance degradation or crashes, Autopatch can automatically pause or roll back the deployment.

Zero-Touch Maintenance: This moves the administrative burden from "packaging and deploying" to "monitoring and reporting," allowing the IT team to focus on higher-value tasks.

4.11.2.3. Decision Success Criteria

Success Criteria	Measurement / KPI	Target Threshold	Validation Method
All Cloud PCs receive Microsoft 365 Apps via Intune and follow the same baseline policies	% Cloud PCs deployed with M365 Apps via Intune	≥ 98%	Intune Apps > Assignment Report; Device install status
Configuration drift is eliminated (policy parity across all provisioning policies)	% devices compliant with M365 configuration profiles (macros, security baselines, settings)	≥ 98% compliant	Intune Device Configuration compliance reporting
No unmanaged Microsoft 365 installations exist	# of devices with unmanaged Microsoft 365 installs detected	5/5	Intune configuration profile.
All Cloud PCs are migrated off the Semi-Annual / Monthly Enterprise channels	% Cloud PCs using Current Channel	≥ 98% within migration window	Microsoft 365 Apps inventory (Intune / M365 admin centre)
Feature parity improves (users get modern features without delay)	“Feature gap” incidents or user escalations related to missing features	Trend downward (baseline to be established)	ITSM analytics, user feedback, service desk categorisation

Update cadence matches Microsoft 365 service evolution	Median time from Microsoft release to availability on Cloud PCs	≤ 14 days (Broad ring)	Autopatch deployment reports / M365 release tracking
Cloud PCs are enrolled on Autopatch and receive updates through ring deployment	% Cloud PCs successfully enrolled into Autopatch	≥ 98%	Autopatch portal / Intune policy assignments
Rings are populated correctly (Test/First/Fast/Broad)	% Cloud PCs assigned to the correct Autopatch rings	100%	Autopatch ring reporting
Updates deploy without significant disruption.	Incident rate caused by M365 Apps updates (crashes, add-in failures, performance regressions)	≤ 2 P1/P2 incidents per quarter	ITSM incident correlation + Autopatch health
Autopatch pauses/rollbacks function as designed	Time to detect and pause/rollback problematic update	≤ 48 hours from detection	Autopatch health monitoring + incident timeline review
Reduced manual effort for patch management	Monthly hours spent managing Microsoft 365 update rings	≥ 70% reduction from baseline	Time-tracking / operational metrics
User productivity remains stable or improves	% of users reporting “no disruption” due to M365 updates	≥ 90% positive	Pulse survey/helpdesk metrics
Microsoft 365 application crash or instability is minimised	Office crash rate per 1000 active users	≤ baseline (improving trend)	Endpoint analytics/crash telemetry
Performance and login experience remain acceptable	Avg. Office app launch time (Word/Outlook/Teams) on Cloud PCs	≤ 10% variance from baseline	Endpoint Analytics / W365 performance metrics
Security patches are applied rapidly to reduce exposure	% Cloud PCs patched within SLA	≥ 95% within SLA window	Autopatch compliance reports
Microsoft 365 Apps remain supported and compliant	% devices running supported M365 Apps build	100%	M365 Apps lifecycle report + Autopatch reporting

4.11.3. Edge as a Service

4.11.3.1. Current State

Edge servicing is currently unmanaged and not audited. The assumption is that Edge is automatically updating on Windows devices.

4.11.3.2. Decisions

4.11.3.2.1.1. Use Autopatch for Servicing

Edge will use the Autopatch infrastructure for staging and the gradual rollout of updates to the environment.

4.11.3.3. Decision Success Criteria

Current State	Decision	Success Criteria	How We Measure It	Evidence / Artifact
Edge updates are assumed to be automatic, unmanaged, and unaudited	Use Autopatch for servicing	Edge updates are deployed via Autopatch rings with controlled rollout (test → broad)	Confirm that Edge update policies and Autopatch ring assignment are applied to scoped devices	Intune/Autopatch policy configuration + ring membership export/screenshot
No staging or measured rollout	Use Autopatch for servicing	Updates successfully progress through rings without excessive failures	Track deployment success/failure rates per ring	Use the Edge dashboard.
No audit trail/visibility	Use Intune for management.	The application telemetry is stored in the cloud.	Report on the current distribution of Edge versions and update compliance.	Console Intune showing versions, use the Graph API to export data.
Unknown time-to-update	Use Autopatch for servicing	Devices update within expected rollout windows	Measure time from release approval to broad deployment completion	Rollout timeline logs/reports
No controlled blast radius	Use Autopatch for servicing	Pilot ring detects issues before the broad ring; the rollback/hold process works	Validate the ability to pause/hold updates and document action	Change record + Autopatch pause/hold evidence
Unclear scope	Use Autopatch for servicing	All managed Windows devices with Edge in scope are included (and exceptions are documented)	Compare device inventory to Autopatch ring membership	Device inventory + exception register
No defined operational process	Use Autopatch for servicing	Roles and processes exist for monitoring, triage, and escalation	Confirm RACI + runbook exists and is used	Runbook + RACI document

4.11.4. Modern Application Servicing

4.11.4.1. Current State

Currently, the store application is disabled on physical Windows devices. Users also lack access to the store application.

4.11.4.2. Decisions

4.11.4.2.1. Disable Microsoft Store user access

End users will be prevented from accessing or interacting with the Microsoft Store application, even if they attempt to launch it. The store application will run in the background.

4.11.4.2.2. Allow Microsoft Store background services

The Microsoft Store application will continue to run in the background to synchronise with Microsoft services. This ensures that installed modern applications and required system components remain up to date.

4.11.4.3. Decision Success Criteria

Decision	Success Criteria	Measurement Method
Disable Microsoft Store User Access	Users are unable to launch or interact with the Store UI.	Attempting to open the Store app results in a "blocked" message or immediate closure.
Allow Store Background Services	Integrated Windows apps and Store-based components update automatically without user intervention.	Verify that apps like Calculator, Photos, or Notepad show recent update history in "Apps & Features."
Modern App Synchronisation	System components remain synchronised with Microsoft services.	Review Intune or Event Viewer logs to confirm successful background sync tasks with the Windows Update/Store service.
Impact on Win32 Servicing	Store background activity does not interfere with standard Win32 application deployments.	Confirm that MSIX or Win32 app installations via Intune proceed without conflicts from the Store service.

4.11.5. Win32 Application Servicing

4.11.5.1. Current State

Currently, the policy around application upgrades is ticket-driven. A business or IT user will request an application upgrade, usually for functionality, and, in rare circumstances, for security updates.

4.11.5.2. Decisions

4.11.5.2.1. Proactively Monitor Common Applications

Monitor applications such as 7-Zip and Remote Help for new versions and security updates. For example, the current data underscores the need to keep a tool like 7-Zip up to date.

Version	Vulnerabilities

25.01	0
25	1
24.09	4
24.08	4
24.07	5
24.06	6

4.11.5.2.2. Repackage New Win32 Applications

In addition to constant monitoring, these applications require repackaging. The process may have minimal requirements, such as a silent installation package, but it still involves manual overhead in building and testing these applications.

4.11.5.3. Decision Success Criteria

Decision	What "Success" Looks Like	Measurable Criteria (KPIs)	Evidence / How to Verify
Proactively Monitor Common Applications	Common, high-risk Win32 apps (e.g., 7-Zip and Remote Help) are monitored continuously, and new versions/security fixes are identified quickly enough to prevent drift and reduce exposure.	Coverage: ≥ 90% of "common apps" list monitored (or 100% of the defined baseline list). Detection latency: New version/CVE identified within one business day of release/notice. Currency: ≥ 95% of Cloud PCs have monitored apps within N-1 (current or previous) versions. Risk reduction: The "Known vulnerable versions" trend decreases month over month for monitored apps (e.g., avoid staying on versions with multiple known vulnerabilities, such as older 7-Zip releases).	Monitoring logs/feeds (vendor release notes/CVE sources). Version inventory reports (Intune app inventory / discovered apps). Compliance dashboard showing version distribution and out-of-date counts.
Repackage New Win32 Applications	When monitored apps release updates, packaging and validation happen consistently with minimal manual friction, and upgrades are deployed safely with rollback paths.	Packaging SLA: New version packaged and ready for pilot within five business days of detection (or faster for critical CVEs). Standardisation: 100% of packaged apps include silent installation and uninstallation, detection logic, and documented installation behaviour. Pilot success: ≥ 95% install success rate in pilot ring within 48–72 hours. Production success: ≥98%	Intune Win32 app objects (install command, uninstall command, detection rules). Packaging checklist sign-off (test cases + outcomes). Intune install status reports (failure codes, device success). Update the record/release notes entry for each package.

	installation success rate in the production ring within 7–14 days of pilot sign-off. Rollback readiness: 100% of updates have a documented rollback/uninstall procedure, and the last-known-good package is retained.

4.11.6. Management as a Service

4.11.6.1. Intune

4.11.6.1.1. Current State

As a cloud-native platform, Microsoft Intune follows a rapid release cadence. Maintaining operational awareness of these service changes is critical to ensuring continued compatibility and leveraging new feature sets.

The primary resource for tracking these changes is the official "What's New in Microsoft Intune" documentation on Microsoft's site. This site provides detailed summaries of monthly service releases, UI changes, and deprecated features.

4.11.6.1.2. Decisions

4.11.6.1.2.1. Bi-Monthly Review Process

Establish a bi-monthly operational review process to evaluate Intune service updates and assess their impact on the Windows 365 environment.

4.11.6.1.2.2. Integrate with Change Management

Integrate Intune feature releases into the existing IT change management framework to ensure stakeholders are notified of significant UI or functional shifts.

4.11.6.1. Decision Success Criteria

Decision Statement	Success Criteria	Metrics / KPIs	Trigger / Input Source
Establish a bi-monthly operational review process to evaluate Intune service updates and assess their impact on the Windows 365 environment.	The bi-monthly review occurs on schedule; the impact assessment is completed and documented; and any required remediation/communications are tracked to closure.	90 % of scheduled reviews completed on time >1# of impactful Intune changes identified 5 Day Avg. time to assess impact <1# of compatibility issues/incidents attributed to unreviewed change	Microsoft Intune release notes / “What’s new in Microsoft Intune”; Microsoft 365 admin message centre (as applicable)

Integrate Intune feature releases into the existing IT change management framework to ensure stakeholders are notified of significant UI or functional shifts.	Significant Intune changes are routed through change management; stakeholders are notified before deployment/impact; change records include risk, test/rollback, and communications.	95% of significant changes with approved change record • Lead time for notifications 5 days • 1 of stakeholder communication sent	Microsoft Intune release notes; internal change calendar; CAB intake (if applicable)

4.11.6.2. Cloud PC Lifecycle Management

The lifecycle of the Cloud PC follows four distinct phases. From provisioning and updates to re-provisioning and decommissioning, Cloud PCs offer features that let users restore or rebuild them, with or without IT assistance.

4.11.6.2.1. Decisions

The integration of Windows 365 and Intune streamlines the end-to-end device lifecycle—from initial provisioning to retirement or hardware transition. By leveraging cloud-based deployment, the organisation can move away from traditional, labour-intensive imaging processes.

Modernising this lifecycle also necessitates a shift in how the organisation handles device end-of-life. In many cases, simply removing access and unassigning the Cloud PC license is sufficient.

4.11.6.2.1.1. Onboarding Process & Provisioning Logic

To ensure consistency and security, the organisation must define an automatic trigger for Cloud PC provisioning.

- **Decision:** Use group-based licensing in Entra ID as the trigger for Cloud PC provisioning.
- **Implementation:**
  - **Licensing:** Licenses will be assigned via Entra ID security groups.
  - **Provisioning Policy:** A specific Intune Provisioning Policy will be targeted to this group, defining the Join Type (e.g., Microsoft Entra Join) and the Network (e.g., Microsoft Hosted Network). Helping trigger provisioning when the user is added to the group.
  - **User Settings:** The "Standard User" vs. "Local Administrator" privilege level will be defined at the policy level based on persona (e.g., Developers vs. General Office Workers).

4.11.6.2.1.2. Offboarding & Grace Period Management

When a user leaves or no longer needs a Cloud PC, the offboarding process must secure their data while preventing accidental loss. Implement a structured de-provisioning workflow leveraging the 7-day grace period for offboarding.

- **Decision:** Implement a structured offboarding workflow that uses Windows 365's 7-day grace period.
- **Implementation:**
  - **Trigger:** Removal of the user from the Entra ID licensed group.
  - **Grace Period:** The default 7-day grace period will be utilised. During this time, the Cloud PC is "de-provisioned" but not deleted, allowing for immediate restoration if the offboarding was triggered in error.
  - **Data Retention:** After the grace period expires, the Cloud PC and all associated data will be permanently deleted. Critical data must be stored in OneDrive for Business or SharePoint to ensure it persists even if the Cloud PC is deleted.

4.11.6.2.1.3. Snapshot & Point-in-Time Restore Strategy

To mitigate risks from malware, bad updates, or user errors, the design requires a recovery mechanism.

- **Decision:** Enable point-in-time Cloud PC restore (snapshots) for both users and admins.
- **Implementation:**
  - **Frequency:** Snapshots will be captured automatically by the service at 12-hour **intervals**.
  - **Retention:** Retention: The system keeps the last 10 restore points for each Cloud PC.
  - **Self-Service:** Enable 'User-initiated restore' in the Windows 365 portal… allowing users to revert their Cloud PC to a previous state without IT intervention.

4.11.6.3. Decision Success Criteria

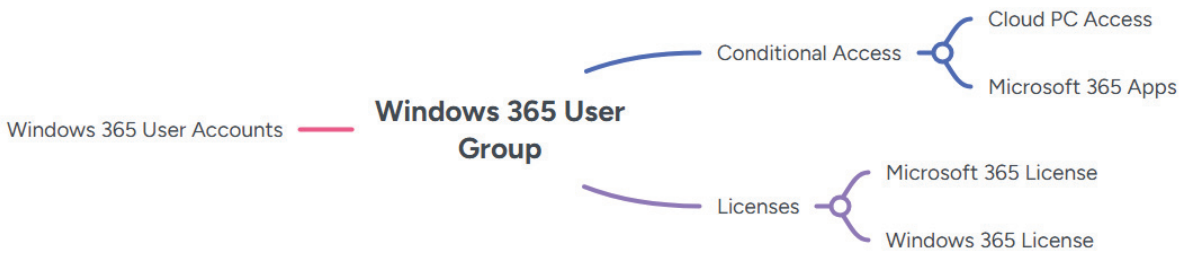
Decision Area	Decision	Success Criteria
Onboarding Process & Provisioning Logic	Use Group-Based Provisioning via Microsoft Entra ID	Cloud PCs auto-provision reliably when users are added to the licensed group. Licenses are assigned correctly via security groups, with no manual intervention required. The provisioning policy targets the correct users and applies the appropriate Join Type and Network settings. The privilege level (Standard vs Local Admin) consistently aligns with persona rules. Manual imaging/provisioning effort and provisioning time are reduced.
Offboarding & Grace Period Management	Structured De-provisioning workflow using 7-day grace period	Removing a user from the licensed group consistently triggers deprovisioning. Cloud PC access is revoked immediately and securely upon group removal. Grace period allows recovery if offboarding was accidental (restore works within 7 days). Automatic deletion occurs after the grace period with no orphaned Cloud PCs. Critical files are stored in OneDrive/SharePoint with no business data loss incidents.
Snapshot & Point-in-Time Restore Strategy	Enable User/Admin-led restore via Snapshots	Restore points exist and match the expected cadence (every 12 hours). At least 10 restore points are consistently available per Cloud PC. Users can complete a self-service restore without admin escalation. Help desk tickets for rollback/recovery scenarios are reduced. Successful recovery

		from malware/corruption/user error is validated through testing.

5. Appendix

5.1. Appendix A: Example Mind Map

5.2. Appendix B: User Group Visualisation



5.3. Appendix C: Technical Definitions

Here is a Technical Definitions section suitable for inclusion in the appendix of your Windows 365 Cloud PC reference architecture document. It defines key terms used throughout the document to ensure clarity for technical and semi-technical readers:

Term	Definition
7-Zip	An open-source file archive utility for compressing and extracting files is often included as a standard tool for handling various archive formats on Windows.
Active Directory	Microsoft's on-premises directory service (Active Directory Domain Services) that stores identities (users, computers) and handles authentication/authorisation in Windows domain networks. It relies on domain controllers to validate credentials and apply domain policies.
Application Protection Policies (APP)	Data protection rules (part of Intune/Microsoft Purview) enforce controls such as preventing data sharing or copying from managed apps. These mobile app management policies help ensure that corporate data in apps (e.g., Office Mobile) remains protected (e.g., by preventing copy-paste to unmanaged apps).
Azure Active Directory (Azure AD)	The former name of Microsoft Entra ID, the cloud-based identity and access management service for managing users, groups, and sign-in access to Microsoft 365, Azure, SaaS apps, etc. Azure AD (now Entra ID) provides single sign-on, Conditional Access, and directory services in the cloud.
Azure Disk Encryption (ADE)	A feature that encrypts the OS and data disks of Azure virtual machines using BitLocker (for Windows VMs) or dm-crypt (for Linux VMs). ADE helps protect data at rest by enabling full-disk encryption, with encryption keys managed in Azure Key Vault.
Azure Monitor	A comprehensive cloud monitoring platform on Azure that collects and aggregates metrics, logs, and diagnostics from Azure and on-prem environments. Azure Monitor enables analysis and alerting to maximise application performance and promptly detect issues across infrastructure and services.
Azure Network Connection (ANC)	A Windows 365 networking option that connects Cloud PCs to a customer's Azure Virtual Network (as opposed to using the Microsoft-hosted network). An ANC allows Cloud PCs to join a specified VNet in your Azure subscription, enabling them to access on-premises resources or custom network configurations.
Azure Subscription	A logical cloud tenant/container in Azure used to provision and group resources (VMs, storage, networks, etc.) and handle their billing. Each Azure subscription is associated with an Azure AD tenant and represents a separate billing unit and boundary for resource access management.
Azure Virtual Network (VNet)	An isolated, software-defined network in Azure that enables Azure resources (VMs, containers, etc.) to securely communicate with each other, the internet, or on-premises networks. A VNet has an IP address space and subnets, and supports features such as network security groups, routing tables, and VPN/ExpressRoute gateways.
Cloud PC	A persistent, cloud-hosted Windows desktop provided by the Windows 365 service. Each Cloud PC is a personal VM assigned to a user, allowing "work-

	from-anywhere" with a full Windows experience accessible via the internet. In this reference design, Cloud PCs are Entra ID-joined, Intune-managed, and remain always on for the user's applications and state.
Co-management	A management approach that bridges Configuration Manager (SCCM) and Microsoft Intune to manage the same Windows device concurrently. In co-management, specific workloads (compliance, app install, updates, etc.) can be offloaded to Intune while others remain under ConfigMgr, facilitating a gradual shift to modern management.
Conditional Access	Entra ID's policy-based access control engine that evaluates signals (user identity, device compliance, location, risk) and enforces requirements before granting access to cloud apps. For example, a Conditional Access policy might require MFA or a compliant device for a user accessing a sensitive app, embodying a Zero Trust "verify explicitly" approach.
Configuration Service Provider (CSP)	An interface in Windows that exposes device configuration settings, allowing MDM platforms like Intune to apply policies remotely. CSPs are used to implement device configurations via MDM by mapping policy settings (e.g. password rules, Wi-Fi profiles) to the underlying OS components. (*Intune uses CSPs and the Settings Catalogue to enforce policies without traditional Group Policy.*)
Credential Guard	A virtualisation-based security feature in Windows that isolates authentication secrets (like NTLM hashes and Kerberos tickets) in a protected virtual enclave so that only privileged system processes can access them. By running LSASS secrets in a VBS container, Credential Guard helps prevent credential theft techniques such as Pass-the-Hash attacks.
Data Loss Prevention (DLP)	Technologies and policies that detect and prevent sensitive information from leaving the organisation in unauthorised ways. In Microsoft 365, DLP can inspect emails, files, chats, and other data, and block or warn about sharing data (such as credit card numbers or confidential information) outside defined boundaries, helping organisations comply with data protection requirements.
Device Compliance	In Intune, device compliance refers to policies and checks that define the minimum security health requirements a device must meet to be considered "compliant." For example, requiring an active firewall, up-to-date antivirus, disk encryption, etc. Compliance status is used by Conditional Access to allow or deny access to resources.
Device Configuration	The management of device settings via modern cloud policies. In an Intune context, Device Configuration involves pushing configuration profiles or Settings Catalogue policies (for settings formerly managed by Group Policy) to enforce settings on Windows devices (e.g. password policies, browser settings) over the internet. This ensures a secure, standardised configuration regardless of user location.
Domain Controller	A server (in Active Directory) that authenticates users and computers and enforces security policies for a Windows domain. Domain controllers store the AD database (NTDS) and handle login requests, Kerberos ticket issuance, and identity data replication. In legacy setups, on-premises domain controllers were required for identity; Cloud PCs in this design eliminate that dependency via Entra ID join.

Entra Connect	A directory synchronisation tool (formerly Azure AD Connect) that links on-prem AD with Microsoft Entra ID (Azure AD). Entra Connect syncs users, groups, and password hashes (optional) from a local Active Directory to the cloud directory. This allows hybrid identity scenarios, ensuring on-prem AD identities exist in Entra ID for Cloud PC assignments.
Enrollment (Intune)	The process of registering a device with Microsoft Intune for management. During Cloud PC provisioning, automatic Intune enrollment occurs; the Cloud PC enrols into Intune's MDM service so policies, apps, and compliance rules can be applied. Once enrolled, the device is managed and monitored by the Intune service.
ExpressRoute	A Microsoft Azure service that provides a private, dedicated network connection from an organisation's on-premises network into Azure datacenters (bypassing the public internet). ExpressRoute circuits offer high-bandwidth, low-latency links that extend on-premises networks to Azure VNets or Microsoft 365, with greater security and reliability. In the Windows 365 context, ExpressRoute can be used for network connectivity to Cloud PCs if needed (e.g. for hybrid join scenarios).
Group Policy Object (GPO)	A set of on-prem Active Directory Group Policy settings that define how Windows systems or user environments should be configured. GPOs can enforce hundreds of policies (security options, software install, script, etc.) on domain-joined PCs. (This Cloud PC design avoids traditional GPOs by using cloud policies via Intune, simplifying management.)
Hyper-V	Microsoft's native Type-1 hypervisor technology for running virtual machines on x86-64 Windows systems. Hyper-V runs underneath the host OS and allows the creation of isolated VMs. It powers Windows features such as Windows Sandbox and Application Guard (which provide virtualisation-based isolation for those security features), and also underpins Azure's VM virtualisation.
Known Folder Move (KFM)	A OneDrive for Business feature that automatically redirects standard Windows user folders, Desktop, Documents, and Pictures to OneDrive cloud storage. KFM helps ensure users' important files are backed up to the cloud and roam across devices. In this design, KFM is enabled via an Intune policy, ensuring that Cloud PC user data is protected in OneDrive.
Log Analytics workspace	An Azure Monitor data store for collecting and querying log data. A Log Analytics workspace houses tables of telemetry (events, audit logs, performance data) from various sources. In the reference architecture, Intune device logs and Entra ID sign-in logs can be streamed to a Log Analytics workspace for advanced monitoring and analytics.
Microsoft Defender Application Guard	A security feature that opens untrusted websites or documents in an isolated Hyper-V container, protecting the host OS from any malicious content. In practice, when a user opens a suspicious URL (in Edge Application Guard mode) or an Office file in Protected View, it runs in a lightweight VM isolated from the corporate desktop. This prevents malware or exploits from escaping the browser/document sandbox.
Microsoft Defender Antivirus	Windows' built-in antivirus solution (formerly Windows Defender) that provides always-on, real-time anti-malware protection. It uses cloud-based threat intelligence and behavioural analysis to detect viruses, spyware,

	ransomware, and other threats, and is centrally manageable via Intune. In this design, Defender AV is active on all Cloud PCs to provide baseline malware defence.
Microsoft Defender for Endpoint	Microsoft's enterprise endpoint detection and response (EDR) platform provides advanced threat prevention, post-breach detection, and automated investigation/remediation on endpoints. Defender for Endpoint uses sensors on Windows 11 Cloud PCs to continuously monitor for anomalous behaviour and attacks, enabling security teams to respond to incidents across the fleet. *(This adds an extra layer beyond the built-in Defender AV.)*
Microsoft Defender SmartScreen	A cloud-based phishing and malware protection service integrated into browsers (Edge/Chrome) and Windows. SmartScreen checks URLs and downloaded files against Microsoft's threat intelligence; if a site or file is known to be malicious or suspicious, it blocks it or warns the user. This provides an "early warning system" against phishing websites and malware downloads on Cloud PCs.
Microsoft Edge	The modern Chromium-based web browser from Microsoft is used as the primary enterprise browser in this architecture. Microsoft Edge integrates with Entra ID for single sign-on and Conditional Access, and supports policies (via Intune) for homepage, extension control, and IE mode for legacy sites. In this design, Edge is configured with security baselines and kept up-to-date (via Autopatch) to serve as a secure gateway to web apps.
Microsoft Entra ID	The new name for Azure Active Directory is Microsoft's cloud-based identity and access management service. Entra ID provides user and device identity, single sign-on authentication, Conditional Access, and directory services for Microsoft 365 and Azure. In this design, Cloud PCs and users are Entra ID-joined, eliminating the need for on-prem AD. (All users must exist in Entra ID to receive a Cloud PC.)
Microsoft Endpoint Manager (MEM)	The former branding (2019–2023) for the unified endpoint management suite, combining Microsoft Intune (cloud MDM) and Configuration Manager (on-prem). Essentially, MEM referred to the integrated management platform for all devices. *Note:* Microsoft has retired the "Endpoint Manager" name; it now simply refers to Intune for cloud management and ConfigMgr for on-premises.
Microsoft Intune	A cloud-based unified endpoint management (UEM) service that centrally manages devices (Windows, macOS, iOS, Android) and enforces security policies. Intune (part of the Microsoft Intune Suite) is used in this solution to automatically enrol Cloud PCs and apply configurations, deploy applications, and ensure compliance. It provides a "single pane of glass" to manage the Cloud PC lifecycle, replacing traditional PC management with internet-based MDM.
Microsoft Purview Information Protection	An integrated set of capabilities to classify, label, and protect sensitive information across an organisation. It includes sensitivity labels that users or automatic rules can apply to documents/emails, which can enforce encryption, watermarking, or access restrictions. In this solution, Purview labels (e.g. "Confidential") could be used to prevent Cloud PC data leakage by requiring encryption or blocking external sharing of labelled content.

Microsoft Store for Business	(Retired in 2023) A service that allowed organisations to curate and distribute applications from the Windows Store to their users. It provided a private app store for enterprises to acquire apps and assign licenses. In this design, modern app deployment is handled via the new winget/Store integration in Intune, as the Windows Store for Business is deprecated. *(The Store for Business concept is mentioned for legacy awareness, but the solution uses the new Store integration with Intune.)*
Microsoft Teams	The Microsoft 365 chat, conferencing, and collaboration application. In the Cloud PC image, Teams is included as part of Microsoft 365 Apps and optimised for Cloud PC use (e.g. AV redirection). Teams enables users to make calls, hold meetings, and collaborate in real time. Windows 365 supports Teams with media optimisations to offload audio/video processing for performance.
Microsoft 365	The subscription suite includes Windows 11 Enterprise, Office 365 productivity apps, and Enterprise Mobility + Security (EMS) features. Microsoft 365 provides an integrated environment for Office apps (Word, Excel, PowerPoint, Outlook, Teams), device management, and security. In this project, Cloud PCs run Windows 365 Enterprise, which is part of M365, and users leverage Office apps and EMS capabilities (Intune, Conditional Access) included with Microsoft 365 E3/E5 licenses.
Microsoft 365 Apps for enterprise	The subscription-based version of the Office desktop apps suite (formerly Office 365 ProPlus) is included in Microsoft 365. It provides Word, Excel, PowerPoint, Outlook, OneNote, Teams, etc., with continuous updates via the Monthly Enterprise Channel. In the Cloud PC base image, Microsoft 365 Apps are pre-installed and activated via the user's M365 license, ensuring users always have the latest productivity tools.
Microsoft 365 Message Center	An admin-facing notification hub in the Microsoft 365 admin portal that publishes announcements about upcoming changes, new features, and maintenance for Microsoft cloud services. IT admins monitor the Message Center to stay informed of updates (for example, new Intune features or Windows 365 service changes) and to plan accordingly. In this design, the IT team has a "proactive rhythm" of reviewing Message Center posts weekly.
Mobile Device Management (MDM)	A modern management approach for devices where a device is remotely managed through an agentless protocol (built-in OS support). Intune uses MDM to apply configurations and policies to Windows 10/11 (and mobile OS) devices over the internet. MDM provides lifecycle management (settings, certs, remote wipe, etc.) without traditional domain join. *(Cloud PCs in this design are managed via Intune MDM rather than via Group Policy, enabling "cloud-only" management.)*
Monthly Enterprise Channel (MEC)	The Office update channel for Microsoft 365 Apps provides monthly feature and security updates on an enterprise-oriented schedule. In this design, Office apps on Cloud PCs are kept current via MEC, meaning users get updates roughly once a month (after initial validation rings), balancing new features with stability. This channel is managed via Intune policies or Autopatch to ensure that at least 90% of devices remain on the latest release.
Multi-Factor Authentication (MFA)	An authentication method that requires a user to present two or more verification factors to gain access (e.g., a password plus a phone verification or biometric). Entra ID Conditional Access policies here enforce MFA for Cloud PC

	sign-ins and other Microsoft 365 access, as an essential part of Zero Trust security. MFA significantly reduces the risk of account compromise by phishing or password guessing.
OneDrive for Business	Microsoft's cloud file storage service for organisations, part of M365. It provides each user with a personal cloud drive (1 TB+ storage) for their work files. In the Cloud PC environment, OneDrive is used with Known Folder Move so Desktop/Documents/Pictures are synced, ensuring user data is backed up and roams with the user. OneDrive integration also enables features like Files On-Demand and secure file sharing with colleagues.
Remote Desktop Client	The Microsoft Remote Desktop client application (available for Windows, macOS, and mobile) is used to connect to Windows 365 Cloud PCs or other remote desktops. It provides a high-performance remote display experience. Users can launch their Cloud PC in a web browser or via this native Remote Desktop client, which uses the RDP protocol to stream the Cloud PC's display to the user's device. In essence, it's the client software that endpoints use to access the Cloud PC.
Remote Help	A cloud-based remote assistance tool in the Microsoft Intune Suite that allows helpdesk staff to remotely view or control a user's desktop (similar to Remote Assistance/TeamViewer). Remote Help is used to support Cloud PC users in a Zero Trust environment; it operates over the internet and can enforce authentication and logging of support sessions. (It requires an Intune add-on license for helpers.)
Role-Based Access Control (RBAC)	An authorisation mechanism that assigns permissions to users based on roles. In Azure/M365, RBAC is used to control admin access – for example, Intune or Azure roles define what actions admins can perform. Defining RBAC roles (e.g. Intune Administrator, Global Reader) ensures least-privilege administrative access to the cloud environment. In the Log Analytics context, RBAC also controls who can read or modify workspace data.
Secure Boot	A UEFI security feature that ensures only trusted, signed bootloaders and OS components are allowed to execute during system startup. Secure Boot prevents unauthorised bootkits or malware from loading in the boot process by verifying digital signatures. In the Cloud PC image (Windows 11 Enterprise), Secure Boot is enabled by default as part of OS hardening (along with VBS/Credential Guard) to establish a trusted boot chain.
Settings Catalog	A collection of all available device configuration settings in Intune's interface, allowing granular policy creation (analogous to Group Policy settings). The Settings Catalogue in Intune includes hundreds of Windows settings (security options, browser settings, etc.) that admins can configure. In this solution, Intune's Settings Catalogue is used to implement fine-grained controls via Device Configuration profiles, replacing traditional GPOs.
Shared Computer Activation (SCA)	A licensing mode for Microsoft 365 Apps that allows Office to activate on a Windows 365 Cloud PC (or other VDI) without consuming a regular device license. SCA is used in non-persistent or multi-user scenarios. In this design, Office is configured with SCA via Entra ID, so if a user has multiple Cloud PCs or sessions, Office apps activate properly for each user session without extra license usage.

Single Sign-On (SSO)	An authentication property in which a user logs in once and gains access to multiple systems without re-entering credentials each time. In this environment, Entra ID provides SSO – when a user is authenticated to their Cloud PC and Entra ID, they seamlessly access Microsoft 365 apps and other resources without additional prompts. SSO improves user experience and reduces password fatigue, while still subject to Conditional Access checks.
Universal Windows Platform (UWP)	The modern app model for Windows apps allows the same app package to run across various Windows 10/11 devices. UWP apps are distributed via the Microsoft Store and run in a sandbox with modern permissions. In this document, VLC (UWP) refers to the UWP version of VLC media player, available from the Microsoft Store and running in a sandbox for security. (UWP apps like VLC are optionally provided via the Company Portal for users.)
Virtualisation-Based Security (VBS)	A security mechanism that uses the Windows hypervisor to create an isolated memory enclave, separate from the standard OS, for sensitive security functions. VBS enables features such as Credential Guard and Device Guard by running parts of the OS (such as LSASS secrets) in a protected virtual context that malware in the main OS cannot tamper with. VBS is enabled on Cloud PCs (Windows 11) to strengthen resistance against kernel-level attacks.
Virtual Private Network (VPN)	An encrypted network tunnel over the public internet that connects a device or network to another network, as if they were directly connected. In Azure/Windows 365 contexts, site-to-site VPNs can connect on-premises networks to Azure VNets for Cloud PC access to on-premises resources. However, this reference design prefers using the Microsoft-hosted network or ExpressRoute/ANC for simplicity, and avoids VPN gateways unless necessary. (If used, Azure VPN Gateway would establish IPsec tunnels to on-prem VPN devices.)
Windows 365	Microsoft's Cloud PC service provides Cloud PCs (persistent Azure-hosted Windows 10/11 desktops) to users as a SaaS offering. Windows 365 handles the orchestration of provisioning, computing, and licensing. Two editions exist: Business (simpler, for small orgs) and Enterprise (integrates with Entra ID/Intune). In this project, Windows 365 Enterprise is used so that Cloud PCs are Entra ID-joined and Intune-managed. Windows 365 allows users to stream their personal Cloud PC to any device, enabling "desktop anywhere" scenarios with predictable per-user pricing.
Windows Autopatch	A cloud service that automates the deployment of updates for Windows, Microsoft 365 Apps, Edge, and Teams across enrolled devices. Autopatch uses a ring-based, gradual rollout (Test, First, Fast, Broad rings) to apply Patch Tuesday updates and feature upgrades in waves, monitoring for issues. In this design, Autopatch is leveraged to keep Cloud PCs and their software up to date without manual admin effort, effectively "managing Windows and Office as a Service" with minimal impact.
Windows as a Service (WaaS)	The Windows 10/11 servicing model delivers regular feature updates (approximately annually) and monthly quality updates, rather than big OS releases every few years. Under Windows as a Service (WaaS), the OS evolves continuously and is maintained in place. For Cloud PCs, this means they are kept on a supported Windows 11 release and receive monthly patches. The reference design emphasises an **"evergreen"** approach: using Microsoft's latest

	gallery image (Windows 11 25H2 in this case) and letting Autopatch/Intune continually update the OS and apps.
Windows Defender Firewall	The host-based firewall built into Windows filters network traffic. It is a stateful firewall that allows or blocks inbound/outbound connections based on rules and profiles. In this architecture, Windows Defender Firewall is enforced via Intune policies on Cloud PCs, with strict rules that prevent unwanted network access between Cloud PCs (isolating them) and allow only necessary traffic, supporting a Zero Trust network posture.
Windows Sandbox	A lightweight virtual desktop environment in Windows 10/11 that allows running applications or opening files in isolation from the host OS. When enabled, Windows Sandbox creates a temporary, throwaway Windows VM that is reset upon closure, so anything done inside does not affect the host system. This is useful for safely testing unknown executables. (In an enterprise Cloud PC, Sandbox could be used by power users or developers to run untrusted utilities without risking the main workspace.)
Zero Trust	A security paradigm that assumes no implicit trust for any user, device, or network – every access request must be explicitly verified ("never trust, always verify"). In practice, Zero Trust involves strong identity verification (MFA), device compliance enforcement, least-privilege access, and segmentation to minimise risk. This Cloud PC design embraces Zero Trust by requiring Entra ID authentication with Conditional Access, verifying device health, removing broad network access (each Cloud PC is isolated), and continually monitoring for anomalies. The result is a modern security posture in which trust is earned through continuous validation rather than assumed by default.