Microsoft Digital Workplace

Solution Suite for Empowering the Modern, Distributed Workforce

---

Executive Summary

Microsoft offers powerful digital workplace solutions with Azure Virtual Desktop (AVD) and Windows 365 Cloud PCs, both powered by Azure.

AVD delivers customizable, scalable virtual desktops with multi-session support, pay-per-use pricing, GPU options, and enterprise-grade security—ideal for complex, variable workloads.

Windows 365 provides simple, persistent Cloud PCs as a SaaS offering with fixed monthly pricing, personalized Windows experiences, and easy management—perfect for hybrid and remote teams. Integrated with Microsoft 365, they enhance productivity, security, and business resilience in modern work environments.

Briefing on Enterprise-Scale Digital Workspaces with Microsoft

Executive Summary

The modern enterprise mandate to support distributed workforces requires a strategic shift toward secure, scalable Desktop-as-a-Service (DaaS) solutions. Microsoft's primary offerings, **Azure Virtual Desktop (AVD)** and **Windows 365 (W365)**, address this by securely streaming resources from the Microsoft Cloud, with a core strategic benefit of centralizing data to reduce the organizational attack surface and enhance compliance.

While both services leverage Azure infrastructure, they serve distinct operational models. AVD is a **Platform-as-a-Service (PaaS)**, offering maximum flexibility, multi-session capabilities, and significant cost-optimization potential through consumption-based pricing, auto-scaling, and Reserved Instances. This makes it ideal for customized, high-density, or cost-sensitive workloads but requires significant IT management overhead. Conversely, W365 is a **Software-as-a-Service (SaaS)** solution providing dedicated, single-session Cloud PCs with predictable, fixed per-user monthly costs and simplified management via Microsoft Intune, suiting standardized desktop needs and organizations with lean IT teams.

For large organizations, the most effective strategy is the adoption of a **Hybrid DaaS Portfolio**, leveraging AVD for its cost-efficiency in pooled environments and W365 for roles requiring operational simplicity and fixed budgets. Architectural success is contingent on a disciplined, multi-layered approach founded on key pillars:

- **Foundational Architecture:** A hub-and-spoke network topology is essential for security and governance, with Azure Firewall controlling egress traffic and RDP Shortpath optimizing user experience by establishing direct UDP connections.
- **Zero Trust Security:** A cloud-native identity model using Microsoft Entra joined VMs is recommended. Security is enforced through Conditional Access policies requiring multifactor authentication (MFA), integration with Microsoft Defender for Endpoint for device compliance, and Microsoft Purview for Data Loss Prevention (DLP) within the virtual session.

- **Modernized Operations:** Application delivery must be modernized by decoupling applications from the OS using **MSIX App Attach**, which significantly reduces image management overhead and improves user logon times. Similarly, user profiles must be containerized with **FSLogix**, which requires high-performance storage like Azure Files Premium or Azure NetApp Files to avoid performance bottlenecks.
- **Financial Operations (FinOps):** Rigorous cost optimization is non-negotiable. This is achieved through AVD's native scaling plans, third-party tools like Login VSI Hydra, and the strategic use of Azure Spot VMs (with a "Delete" eviction policy) for burst capacity. Governance is enforced through Infrastructure as Code (IaC) for consistent deployments and resource tagging.
- **Migration:** Transitioning from legacy VDI platforms must be treated as a modernization effort. A prerequisite for success is the upfront investment in application compatibility assessment and conversion to the MSIX format to avoid carrying legacy operational burdens into the cloud.

Strategic Overview: AVD vs. Windows 365

Microsoft offers two distinct DaaS solutions that, while built on similar technologies, cater to different enterprise needs regarding cost, management, and flexibility.

Core Architectural Models

- **Azure Virtual Desktop (AVD):** A PaaS solution that grants the customer complete control over the virtual desktop environment. This includes managing the operating system (Windows Enterprise multi-session, single-session, and Windows Server), VM sizes (including GPU-enabled instances), storage configurations, and scaling policies. Its key differentiator is support for multi-session Windows, allowing multiple users to share a single VM, which is a primary driver of cost-efficiency.
- **Windows 365 (W365):** A SaaS solution that abstracts away infrastructure management, which is handled entirely by Microsoft. It delivers a personalized, persistent, single-session Windows 10 or 11 Enterprise desktop (Cloud PC) to each user. Management for the Enterprise edition is fully integrated with Microsoft Intune. W365 is designed for operational simplicity and predictable, fixed per-user, per-month subscription costs.

Comparative Analysis

The choice between AVD and W365 depends on a trade-off between cost, control, and complexity.

Feature/Dimension	Azure Virtual Desktop (AVD)	Windows 365 Enterprise (W365)
Underlying Model	Platform as a Service (PaaS)	Software as a Service (SaaS)
Resource Sharing	Multi-session (Pooled) and Single-session (Personal) supported	Dedicated Single-session (Persistent Cloud PC)
Management Complexity	High (Customer manages OS, VM size, scaling, network, identity, storage)	Low (Microsoft manages infrastructure; customer uses Intune for policies)
Cost Driver	Consumption-based (VM runtime, storage, networking). Optimized by auto-scaling, Reserved Instances, and Spot VMs.	Predictable Per-User, Per-Month subscription cost. Fixed regardless of usage.
Primary Use Cases	Highly customized apps, high-density environments, cost-sensitive scaling, legacy app support, dev/test, GPU workloads.	Standardized desktops, rapid onboarding (seasonal staff), BYOD scenarios, fixed budget predictability, lean IT teams.
Image Management	Full support for custom images, managed via Azure Compute Gallery and Azure	Supports Microsoft-provided images or custom images (limit of 20 per tenant). Business

	VM Image Builder.	version does not support custom images.
User Profiles	Requires FSLogix profile containers stored on a central SMB share (Azure Files or Azure NetApp Files).	"Native" user profiles stored directly on the Cloud PC's C: drive. FSLogix is not used.

The Hybrid DaaS Portfolio Strategy

For large enterprises, the most strategic approach is a **Hybrid DaaS Portfolio**. This model uses both AVD and W365 to cater to different user personas and business requirements.

- **AVD** is deployed for high-density, pooled user groups where its sophisticated auto-scaling and multi-session capabilities can deliver significant cost savings (up to 58% lower than W365).
- **W365** is assigned to users who benefit from a persistent, dedicated desktop, such as executives or specific knowledge workers, or for scenarios like mergers and acquisitions where rapid, simple onboarding is paramount.

This hybrid model allows an organization to balance the operational simplicity and predictable costs of SaaS with the granular control and cost-efficiency of PaaS.

Foundational Architecture and Connectivity

Enterprise-scale AVD deployments must be built on a secure and scalable network foundation, adhering to architectural best practices like the hub-and-spoke topology.

Network Topology: Hub-and-Spoke

- **Hub VNet:** This central virtual network contains shared services, including connectivity gateways (ExpressRoute or VPN), centralized security appliances like Azure Firewall, and identity services (domain controllers).

- **Spoke VNets:** These virtual networks contain the AVD session hosts and their associated storage. Spokes are peered with the Hub VNet to access shared services and on-premises resources. This design centralizes security, simplifies management, and allows for scalable growth across multiple Azure subscriptions.

Network Security Controls

- **Logical Segmentation:** Subnets should be logically segmented, with Network Security Groups (NSGs) applied to control traffic flow between them. NSGs act as stateful firewalls using 5-tuple rules (source/destination IP, port, protocol) to enforce access controls.
- **Centralized Egress Control:** It is a best practice to force all outbound internet traffic from session hosts through a central **Azure Firewall** located in the Hub VNet using User-Defined Routes (UDRs). This allows for comprehensive inspection, threat detection, and filtering of all egress traffic.
- **Dedicated WAN Links:** For hybrid connectivity, **Azure ExpressRoute** is recommended over Site-to-Site VPNs. ExpressRoute provides a private, dedicated WAN link that does not traverse the public internet, offering greater reliability, performance, and security.

Performance Optimization with RDP Shortpath

RDP Shortpath enhances the user experience by establishing a direct, UDP-based transport between the client and the session host, bypassing the AVD Gateway. This reduces latency and improves connection reliability. It operates in two primary modes:

- **Managed Networks:** Establishes a direct UDP connection over a private link like ExpressRoute or a VPN. This requires enabling the RDP Shortpath listener on session hosts (default port 3390) and ensuring firewalls permit the direct connection.
- **Public Networks:** Establishes a direct UDP connection over the public internet using STUN to discover public IP addresses and ports, or a relayed connection using TURN if a direct path is blocked (e.g., by a symmetric NAT). This requires session hosts to have outbound UDP connectivity to STUN/TURN services.

The implementation of RDP Shortpath requires careful network configuration to allow

direct client-to-host UDP connectivity, especially across a wide dynamic port range (49152–65535), without creating unintended security vulnerabilities.

Identity, Access, and Zero Trust Security

A Zero Trust security posture is fundamental to protecting enterprise digital workspaces. This approach eliminates trust based on network location and instead validates every access request.

Identity Models

Azure Virtual Desktop requires all user identities to be discoverable through **Microsoft Entra ID**.

- **Hybrid Identity:** Users managed in on-premises Active Directory Domain Services (AD DS) are synchronized to Microsoft Entra ID via Microsoft Entra Connect. For this model to function correctly, the User Principal Name (UPN) or Security Identifier (SID) must match between AD DS and Entra ID. Session hosts can be hybrid joined.
- **Cloud-Only Identity:** This model is fully supported with **Microsoft Entra joined VMs**. Users are created and managed directly in Entra ID. This is the recommended approach as it eliminates dependencies on on-premises infrastructure and legacy authentication protocols.

Secure Authentication and Access Control

- **Conditional Access (CA):** Microsoft Entra Conditional Access is the core tool for enforcing Zero Trust. Policies must be configured to require **multifactor authentication (MFA)** for all users accessing AVD or W365.
- **Single Sign-On (SSO):** SSO using Microsoft Entra authentication is recommended for both Entra joined and hybrid joined session hosts to provide a seamless user experience.
- **Passwordless Strategy:** Enterprises should promote in-session passwordless authentication using Windows Hello for Business or FIDO keys.
- **Privileged Access:** Privileged roles should be protected with **Privileged Identity Management (PIM)**, which provides time-bound, approval-based

elevation instead of permanent admin rights.

- **Just-in-Time (JIT) Access:** JIT VM access in Microsoft Defender for Cloud should be used to lock down inbound management ports (RDP/SSH), opening them only after workflow approval. For remote management, **Azure Bastion** is recommended as it provides secure RDP/SSH connectivity through the Azure portal over TLS without exposing public IP addresses.

Endpoint Protection and Data Loss Prevention

- **Microsoft Defender Integration:** All AVD session hosts and W365 Cloud PCs must be onboarded to **Microsoft Defender for Endpoint**. This provides threat and vulnerability management, attack surface reduction, and automated remediation capabilities.
- **Device Compliance:** Microsoft Intune compliance policies must be used to enforce a security baseline on devices (requiring features like encryption and secure boot). A Conditional Access policy should then be used to block access from non-compliant devices.
- **Data Loss Prevention (DLP): Microsoft Purview Endpoint DLP** should be enabled to prevent data exfiltration. DLP policies can be configured to block sensitive data from being copied to unauthorized devices, restrict printing, and control access to removable media.

Image Management and Application Delivery

Modernizing application delivery is critical to realizing the operational benefits of DaaS, primarily by decoupling applications from the operating system image.

Standardized Image Creation

- **Azure VM Image Builder (AIB):** This managed service, built on HashiCorp Packer, automates the creation of standardized "golden images" for AVD. AIB ensures that all images include predefined security settings, corporate configurations, and necessary software, promoting consistency across deployments.

Dynamic Application Delivery with MSIX App Attach

MSIX App Attach is a modern application delivery technology that separates applications from the OS and delivers them dynamically to user sessions.

- **How it Works:** MSIX-packaged applications are stored in a VHD, VHDX, or CimFS virtual disk on a network share. At user logon, this disk is mounted to the session host, and the application appears to the OS and user as if it were locally installed.
- **Key Benefits:**
    - **Reduced Image Sprawl:** Decoupling apps from the OS drastically reduces the number and complexity of golden images that IT must maintain.
    - **Simplified Application Lifecycle Management (ALM):** Applications can be updated and managed independently of the OS image.
    - **Improved Performance:** This approach can reduce the OS footprint by 25% and accelerate user logon times by up to 40%.
    - **Enhanced Security:** Containerization isolates the application, user data, and the OS.
- **Critical Dependency:** The performance of MSIX App Attach is heavily dependent on the latency and IOPS of the underlying storage share where the application disks are hosted.

Performance, User Experience, and Storage

A high-quality user experience depends on a balanced architecture across network, compute, and storage.

FSLogix Profile Containerization

FSLogix is the standard for profile management in AVD. It captures the entire user profile into a VHD/VHDX container stored on a central SMB file share. This ensures that users receive a consistent, personalized experience regardless of which session host they connect to in a pooled environment.

High-Performance Storage Architecture

Because both FSLogix profiles and MSIX App Attach packages are mounted over the network, the performance of the underlying storage solution is critical.

Storage Solution	Description	Best Fit
Azure Files Premium	A fully managed, highly available, enterprise-grade SMB file share service optimized for random access workloads. It offers single-millisecond minimum latency.	General-purpose workloads, standard office environments, and task workers with moderate I/O demands.
Azure NetApp Files (ANF)	A fully managed, enterprise-grade NAS service built on NetApp's bare-metal hardware. It is engineered for the most demanding, high-performance, low-latency workloads, offering sub-millisecond latency.	Power users, IO-intensive applications, large-scale deployments, and environments susceptible to "login storms."

Proactive Monitoring and Reporting

- **Azure Native Tools: Azure Monitor** and **Azure Virtual Desktop Insights** are essential for monitoring the health and performance of the AVD environment. They provide dashboards and collect diagnostics, performance counters, and event logs from session hosts and AVD service components.
- **Synthetic Transaction Monitoring:** For large-scale environments, proactive monitoring with tools like **Login Enterprise** is recommended. These tools use virtual users to continuously execute business workflows and measure end-user experience (EUX), detecting performance deviations and application failures before they impact real users.
- **Performance Metrics:** Key metrics to monitor for troubleshooting user experience issues include Input Delay, Frame Rate, RDP Round-Trip Time

(RTT), and resource utilization (CPU, memory) on the session hosts.

Cost Optimization and FinOps

Managing cloud spend is a primary challenge for enterprises. A successful AVD deployment requires disciplined financial operations (FinOps).

AVD Auto-Scaling

The largest source of cost waste in AVD is idle session hosts. AVD's native **scaling plans** automate the process of powering VMs on and off based on schedule and user demand.

- **Load Balancing Algorithms:**
  - **Breadth-First:** Distributes users across all available session hosts to optimize user experience. Recommended during ramp-up periods.
  - **Depth-First:** Saturates one session host at a time before moving to the next. This is more cost-effective as it allows unused hosts to be deallocated sooner. Recommended during peak and ramp-down periods.
- **Third-Party Tools:** Solutions like **Hydra by Login VSI** provide advanced auto-scaling, image management, and user management features to further optimize costs and reduce administrative effort.

Azure Spot Virtual Machines

Azure Spot VMs offer access to unused Azure capacity at a significant discount. They are suitable for workloads that can handle interruptions, making them a good option for providing burst capacity in AVD scale sets.

- **Critical Configuration:** When using Spot VMs in a scale set, the **eviction policy must be set to "Delete."** This ensures that when an instance is evicted, its underlying managed disk is also deleted, preventing the accumulation of storage costs and avoiding hitting instance quota limits.

Governance through Infrastructure as Code (IaC)

- **IaC for Consistency:** Deploying AVD resources using IaC tools like **Bicep** or ARM templates is mandatory for enterprise-scale environments. It ensures that deployments are repeatable, standardized, and consistently configured, minimizing human error.
- **Tagging for Visibility:** A robust resource tagging strategy, enforced through IaC, is essential for cost visibility. Tagging allows costs to be accurately attributed to specific business units or projects, enabling financial chargeback and accountability.

Migration from Legacy VDI

Migrating from platforms like Citrix or VMware Horizon to AVD is a strategic modernization effort that should follow a structured, phased approach.

Phased Modernization Approach

1. **Assessment:** Evaluate the current environment, document user and application requirements, and establish performance and security baselines.
2. **Design:** Develop the target AVD architecture, including the hub-and-spoke network, identity model, and tiered storage solution for FSLogix.
3. **Build:** Provision the Azure infrastructure using IaC and create golden images with Azure VM Image Builder.
4. **Migration:** Transition users and data. Tools like **Azure Migrate** can assist with VM migration. User profiles from legacy systems can be migrated into the FSLogix container format using appropriate tools.
5. **Optimization:** Implement continuous cost management, modern application lifecycle management, and ongoing security monitoring.

Prerequisite: Application Modernization

A common failure in VDI migrations is carrying legacy operational burdens into the new environment. The key to unlocking the agility and reduced overhead of AVD is to decouple applications from the OS.

- **Mandatory Workstream:** The conversion of applications to the **MSIX format** for use with App Attach must be treated as a mandatory prerequisite. If this step is

skipped, the organization will fail to eliminate image sprawl and will continue to face the high administrative costs associated with managing multiple monolithic golden images.

Key Insights and Quotations

"Hydra was the missing layer in our AVD setup; imaging used to take hours, now it takes minutes." — **Infrastructure Architect, Global Retailer**

"The self-service portal and automated scaling just work. My team saves time every single week." — **Senior IT Admin, European Finance Org**

"We were shocked how much Hydra does out-of-the-box. The platform is powerful." — **VDI Team Lead, Global Pharma Company**

"In M365, identity *is* the new perimeter. Many attacks start with stolen credentials... Passwords alone are not enough." — **Arctic IT, "Best Practices for Cloud Security with Microsoft 365"**

"Zero Trust isn’t a product: it’s a security posture. You should treat Zero Trust like a healthy lifestyle change for the whole organization. The new security mantra should be “Never trust, always verify” across all users, devices, and sessions." — **Arctic IT, "Best Practices for Cloud Security with Microsoft 365"**