White paper

Microsoft Intune & worXpace

Better together for Complete Workspace Management

Summary

Microsoft Intune is designed for managing and securing devices in the cloud. It helps IT teams set up new devices, push security settings, and make sure each device follows company rules. But Intune has limits. It doesn't work well offline, doesn't apply changes right away, and struggles with complex app setups or giving users much control and basically stops managing after the policies have been applied.

That's where **worXpace** comes in.

WorXpace is a cloud based system that improves the user workspace. It works with Intune, not against it. While Intune secures the device, worXpace makes sure the user gets what they need, quickly, easily, and without delay. It adds real-time updates, better app delivery, offline support, and a smart self-service portal for users.
With worXpace:

- IT can send any tasks or apps instantly
- Users can install apps themselves, instantly, from a user-friendly catalog, without the need for administrative privileged.
- Devices and User sessions remain managed even when offline
- Personal laptops (BYOD) can get a full workspace without heavy control
- Apps can be deployed in many formats, including legacy and virtual apps

WorXpace also personalizes the user experience. It changes settings and tools based on who the user is, where they are, or what device they're using. And it does all this without interfering with the security that Intune enforces.

Together, Intune and worXpace form a full solution:

- Intune manages the device
- WorXpace manages the user workspace

This combo reduces IT workload, makes users more productive, and works well in modern, flexible workplaces. IT teams gain speed and control. Users gain freedom and ease.
In short: **Intune + worXpace = Secure devices + Happy users.**

Introduction

Microsoft Intune has become a popular solution for modern endpoint management, excelling in areas like security policy enforcement, device compliance, and cloud-based provisioning. However, IT administrators know that no single tool covers every need. Intune's strengths in baseline security and device management come with certain gaps, especially around real-time responsiveness, flexible application delivery, offline operation, and user-specific customization. **This paper explains Intune's strengths and limitations, then shows how worXpace fills each gap to create a seamless, comprehensive workspace management environment.**
The goal is a fact-driven, practical look at why Intune and worXpace together can offer more than Intune alone, sharing minimal areas of best practices, and no direct competition.

Intune's Strengths in Device Management

Microsoft Intune is a cloud-based unified endpoint management (UEM) service that shines in core device management tasks. IT administrators and CIOs value Intune for several key capabilities:

- **Baseline Security Enforcement:** Intune allows you to push security baselines and configurations to ensure every managed Windows device meets your organization's security standards. For example, you can enforce BitLocker encryption, firewall settings, and password policies uniformly. These **security baselines** are Microsoft-recommended sets-of-settings that harden devices against threats. Intune's tight integration with Azure Active Directory (Microsoft Entra ID) also enables **Conditional Access** based on device compliance. Only devices that *meet* the defined requirements (e.g. not jailbroken, up-to-date OS, etc.) are deemed compliant and allowed to access corporate resources. This baseline security coverage is critical for protecting data in today's mobile workforce.
- **Device Compliance & Policy Management:** Intune's compliance policies let you define rules and checks on devices (such as requiring antivirus, OS version, or no admin unlock). Devices report their compliance status to Intune continuously. You can configure automatic actions for non-compliant devices (like sending the user a warning or locking email access) and feed compliance status into conditional access for real-time risk mitigation. In short, Intune is very effective at **evaluating device posture** and ensuring each machine remains within IT's allowed policy, a foundation for zero-trust security.
- **Cloud Provisioning and Autopilot:** Intune simplifies provisioning of new machines through **Windows Autopilot**. IT can drop-ship laptops to employees and have them set up with corporate profiles, apps, and settings automatically at first login, without manual imaging. This cloud-driven provisioning saves time and ensures every device is configured consistently. Intune also manages configuration profiles (device settings, Wi-Fi/VPN profiles, certificates, etc.) centrally. From a CIO perspective, Intune reduces the need for on-premises infrastructure like Active Directory GPO for basic configuration, it handles those tasks through the cloud.
- **Basic Application Deployment:** Intune can deploy standard applications to Windows endpoints. It supports Windows *line-of-business* installation files and the Microsoft Store for Business. Common installer formats like MSI and MSIX are natively supported, as well as wrapping Win32 executables into Intune's package format. For example, an admin can upload an MSI or packaged EXE and push it to a group of devices or make the app **available** for self-service install via the Intune Company Portal. For *lightweight, common apps* (especially modern apps or simple MSIs), Intune's app deployment is adequate and gets the job done.

To summarize, **Intune is excellent for getting devices enrolled, secured, and under compliance**, with a solid baseline of app distribution. These strengths make it a powerful platform for device-centric management. However, many IT professionals have discovered that when it comes to predictability, the *user's workspace experience* and certain advanced scenarios, Intune alone can be limiting. Below, we outline some common gaps.

Where Intune Falls Short: Common Limitations

Intune's cloud-native approach and focus on device-level control mean that some aspects of day-to-day workspace management are less predictable or flexible. IT admins often encounter the following limitations in an Intune-only environment:

- **Unpredictable Policy Timing:** Intune does **not guarantee real-time policy application**. Managed Windows PCs typically check in with the Intune service on a schedule (about every 8 hours by default). While Intune can send push notifications to prompt a device sync when a new app or policy is assigned, in practice the timing can range from immediate to a few hours. If a device is offline or misses the notification, it won't apply changes until the next periodic check-in. This means there's inherent lag and uncertainty, for example, if you urgently deploy a configuration fix or a critical app update, some users might receive it right away, but others might not get it until much later in the day. This *delay* can frustrate IT and users alike, and makes troubleshooting or time-sensitive changes more difficult.
- **Limited Application Delivery Flexibility:** Intune's app deployment works best for standard installers and Store apps, but it **struggles with less common delivery methods**. You cannot directly deploy Microsoft App-V virtual applications through Intune (ConfigMgr could, but Intune does not). If you rely on App-V sequences for legacy apps, Intune offers no native support. Similarly, Intune has no built-in mechanism to leverage package managers like Chocolatey or to deliver apps in a *packageless* fashion (e.g. running an app from a network share, a web-app with dependencies or delivering just a shortcut). Every Win32 app must be prepared (wrapped into an .intunewin package with silent install and detection logic), which adds overhead. There's also no dependency management or complex upgrade orchestration in Intune, it's one app/package at a time. In short, Intune provides a basic pipeline for application installs, but it lacks the flexibility to handle *rich application delivery scenarios* such as virtual apps, on-demand streaming, orchestrated installs of enterprise apps, or mixing multiple installation technologies.
- **Minimal Offline Use:** Because Intune is cloud-based, it assumes devices have regular internet connectivity. If a user's device is offline (traveling, home with no internet, etc.), Intune cannot contact it to push new policies or apps. Many Intune policies only apply during online check-in, and app installations require an internet connection to download the package from Intune's service. There is no offline cache of pending changes beyond what the Windows OS might do with certain policies. This means Intune-managed laptops are **highly dependent on connectivity**, a problem for field workers or travelers. While users can of course use already-installed applications offline, these applications, nor other components within the user's session, will not react to changing circumstances. There's also the risk that a device that stays offline too long falls out of compliance (for example, if it misses a required update). In summary, Intune's management *does not gracefully extend to offline scenarios*.
- **Limited Self-Service for Users:** Intune's idea of self-service is the **Company Portal** app, where users can install applications that IT has published as "available." This is useful, but it's fairly minimal, it lists apps and that's about it. There's no self-service for requesting other resources (like access to a network share or a printer etc.). Another limiting factor that

makes the Company Portal unappealing is its slow response. After selecting an application from the portal, it can take several hours before the app is actually available to the user.

These limitations are not failures of Intune, they stem from its design focus. Intune is **excellent for managing devices at scale** and enforcing compliance, but it doesn't attempt to be a full **user workspace management** or **user environment** solution. To bridge these gaps, organizations often look to complementary systems. **This is where worXpace comes in.**

How worXpace Fills the Gaps

WorXpace is a cloud-based workspace management and application delivery platform (from AppiXoft) specifically designed to shape the digital user workspace and as such complements device management solutions like Intune. In an Intune-managed environment, worXpace acts as a smart layer on top, handling fine-grained workspace configuration, on-demand application delivery, offline operation, and user self-service, all in ways Intune alone cannot. Importantly, worXpace doesn't replace Intune's functionalities; instead, it augments Intune by focusing on what happens *after* the device meets basic compliance. Here's a look at how worXpace fills each gap:

Real-Time, Precise Policy Application

One of worXpace's core strengths is **real-time workspace management**. WorXpace was built to apply changes immediately and predictably, rather than relying on infrequent polling. In fact, worXpace's agent uses techniques inspired by online gaming to propagate updates instantly to online clients. Concretely, the worXpace client maintains a constant sync with the cloud service: by combining frequent checks for updates with receiving **push notifications for immediate changes** when real-time updates are enabled. The result is that when an IT administrator makes a change, such as publishing a new application or altering a configuration, users get the update almost immediately, often within seconds if they are online. This contrasts with Intune's multi-hour (or sometimes multi-day) device sync cycle, eliminating the uncertainty.

For example, imagine you need to deploy a critical browser plugin update to all users due to a zero-day exploit. With Intune alone, you might create a policy or script and then wait, hoping devices check in soon (or manually prompt users to sync). With worXpace, you would publish the update in worXpace, and the agent on each PC would **either fetch it within minutes or get an instant push** if you've enabled that feature. Users might receive a notification or see the change applied without delay. This **precise timing** means IT can push changes (even within a user's session) knowing they will take effect promptly, which is ideal for time-sensitive fixes or coordinating rollouts during maintenance windows. It brings a level of control and responsiveness that simply isn't achievable with Intune's asynchronous model.

Moreover, worXpace can apply many changes **at runtime without forcing logouts or reboots**. Intune often relies on user logon or device restart to enforce certain policies (much like old Group Policies). WorXpace can adjust the user's environment on the fly, for instance, mapping a network drive or printer when a user connects to a specific network, or changing an application setting for the user in real-time, making use of the many '*session events*' worXpace offers, like e.g. Application Start, User Idle, Session Unlock, etc. This dynamic control greatly enhances IT's ability to fine-tune the workspace experience throughout the day, rather than only at login or computer startup.

Flexible Application Delivery Methods

WorXpace was designed with *application delivery flexibility* in mind. It supports a wide range of application types and deployment methods natively, going well beyond Intune's scope. With worXpace, you can centrally manage and deploy traditional MSI installer packages, modern MSIX packages, Microsoft App-V virtual applications, and even Chocolatey packages, all from one interface. The system includes tools to handle "generically" installed apps too (like a simple setup.exe that isn't MSI/MSIX), converting them into managed entities. In essence, **worXpace**

speaks the language of every major Windows app format, freeing you from repackaging everything into a single format.
For example, if your environment still uses an App-V package for an old ERP client, Intune alone can't deploy that. WorXpace, however, can deploy App-V applications easily as part of its normal operations. Likewise, if you want to leverage the extensive repository of community software in Chocolatey, worXpace can integrate those packages into your workspace. An admin could specify a Chocolatey package (say, 7zip or Notepad++) and worXpace will handle installing it on target devices, **fully managed and tracked**. This "any app, anywhere" capability is a huge boost to IT productivity: you're not forced to manually repackage things or stick only to MSI/MSIX.
WorXpace also provides an *intelligent application management layer.* It can even handle post-install steps with standard actions or custom scripting so that the app is ready for use without extra admin effort. In practical terms, deploying a new application or update via worXpace is extremely fast, often just a few clicks to add the package, after which worXpace takes care of preparation and distribution.
Another advantage is **application composition and lifecycle**. WorXpace lets you chain and group applications with dependencies, something Intune doesn't do natively. For example, you might have a base application with prerequisites and an add-on module that should be install ed in a strict order. In worXpace, you could graphically design these relationships (*Application Composition* feature) so that the user's system always ends up with a working combination. Upgrades and uninstallations are also coordinated by worXpace's agent, which watches the system to prevent conflicts. In short, worXpace gives you enterprise-grade application delivery management, covering legacy, modern, and even virtual apps, all under one roof. This fills Intune's gap by letting you deliver *any type of application in the most appropriate way*, rather than being constrained to Intune's somewhat limited methods.

Offline Resilience and Autonomy

Unlike Intune, worXpace is built to handle offline scenarios gracefully. Once a device has the worXpace client installed and has performed an initial sync with the cloud, it can operate **fully offline for extended periods**. WorXpace syncs all the necessary "runtime data" (application definitions, scripts, context rules, etc.) and caches it securely on the device. After that, the worXpace client becomes *self-sufficient*: it can carry out all configured tasks, apply settings, and even continue to manage applications and user settings in changing conditions **without an active internet connection**. In the words of the worXpace documentation, once the data sync is done, the client software is *completely self-sufficient* and "will be able to perform any tasks and start any applications, as defined by the administrator," needing the cloud only for actions that explicitly require online access (like downloading a new app package on demand).
Consider a user who is frequently on the road. With worXpace, any applications or workspace settings that were delivered while online will continue to function offline. If the user reboots their laptop on an airplane, there's confidence that critical configuration (like logon scripts, environment variables, restrictions, etc.) are applied consistently, online or offline. This offline resilience complements Intune perfectly: Intune handles things like device compliance (which mostly matters when the device is online trying to access resources), while worXpace ensures the workspace environment is robust in any network condition. For example, Intune might not be able to revoke a policy on a laptop that hasn't connected in days, but worXpace can at least keep that laptop's workspace functioning as last configured, so the user isn't blocked from doing their job due to lack of

internet. As soon as the laptop reconnects, both Intune and worXpace sync up to apply any new rules. It's a best-of-both-worlds scenario for distributed workforces.

Personalized & Contextual User Workspaces

WorXpace truly shines by providing **precise, context-aware workspace management** that adapts to each user's needs, something Intune doesn't attempt to do. With worXpace, administrators can define fine-grained rules (using contexts, actions, scopes and criteria in worXpace) that tailor the workspace per user, group, device, location, network, time of day, and more. The system was designed on the principle of *removing limitations for both admin and user* so that anything is possible in terms of customization. For the IT admin, this means instead of hard-coding a configuration for all, you can say "if user is in Finance department, map drive X; if in Engineering, map drive Y" or "only apply this setting on laptops, not desktops," etc. WorXpace evaluates these conditions in real time and adjusts the user's environment accordingly.

From the **user's perspective**, this yields a more personalized experience. Their workspace is composed of the applications and settings they need for their role and preferences, not a generic stack of everything IT could imagine.

Beyond applications, worXpace can personalize **settings and configurations** per user. For instance, you might use worXpace to deliver certain registry settings or environment variables only for specific teams or when certain conditions are met (e.g., user is working from home vs. in office). Traditional group policies could do some of this, but Intune's modern management doesn't have an equivalent easy mechanism, worXpace fills that void with a rich context engine. This precise targeting means the workspace can adapt: a developer gets a different workspace than a salesperson and different from the kiosk in the lobby, for example. All of it is centrally defined and dynamically applied by worXpace. The result is a more **personal and efficient workspace** for end-users, and less one-off tweaking by IT admins.

Importantly, **none of this conflicts with Intune**. Intune still provides the base device state (OS configuration, compliance, etc.), and worXpace layers user-centric settings on top. If Intune sets a security policy (like disabling a USB drive), worXpace will not override that, security remains intact. WorXpace simply handles the *userland* configuration that Intune leaves untouched, ensuring each user's environment is optimal for them.

Intuitive Self-Service via Service Point

Perhaps one of the most visible advantages for end-users (and a relief for IT support teams) is worXpace's **Service Point**, essentially a user friendly *corporate app store*. The worXpace Service Point gives users an interface to help themselves to applications and other IT-provided services on demand. IT can publish a catalog of optional applications, users can browse this catalog (organized by categories, with search functionality) and install what they actually need, when they need it. The Service Point operates in real-time, meaning the moment a user selects an application to install, worXpace will immediately deliver it to their device, no waiting involved!

For example, consider a new employee who realizes they need a diagramming tool like Visio, but their laptop didn't come with it. With Intune alone, if Visio wasn't pushed by IT, the user would have to request it and wait for IT to deploy it (or for the next Intune sync). With worXpace Service Point, that user could open the Service Point, find "Microsoft Visio" (assuming IT published it as an available service), and click to install. Within seconds, worXpace installs Visio on their machine. The

key is **empowerment and speed**, users get what they need quickly, and IT is freed from performing routine app installs one by one.

The Service Point isn't limited to just apps. As the name suggests, you can offer various *services* through it. This could include things like requesting access to a specific network drive or printer etc. WorXpace lets you publish these in the same catalog alongside apps. For IT admins, this means you can centralize user-facing offerings in one convenient place.

Crucially, like the Intune Company Portal, the Service Point catalog is curated by the administrator. IT still controls what appears there and who sees what (you can target certain optional apps to certain user groups). This ensures compliance and security are maintained, users can't install random software, only the choices IT has pre-approved. But within those choices, the **user has freedom** to tailor their environment. This approach leads to leaner initial deployments (since you don't have to give everyone every app up front) and happier users who feel in control of their tools. As one summary of Service Point benefits notes, it results in *decreased IT workload, lower costs, a more efficient base image, and higher overall service level*. It's a win-win scenario: IT provides a safe framework for self-service, and users actively participate in customizing their workspace.

In contrast, Intune's Company Portal is a much more basic app catalog that, while useful, doesn't operate in real-time and doesn't extend to things beyond software. WorXpace's Service Point is a modern, user-friendly interface that *brands the IT department as an enabler rather than a gatekeeper*. By complementing Intune with Service Point, organizations can significantly improve user satisfaction and reduce the mundane tasks that IT staff have to handle (since users can handle many of them on their own).

Managing Mixed AAD, AD, and BYOD Environments

In many real-world organizations, especially in education, healthcare, or project-based teams, you're not dealing with just one kind of device setup. You might have:

- Company-owned laptops joined to **Azure AD (AAD)** through Microsoft Entra ID
- Older systems still bound to traditional **Active Directory (AD) domains**
- A growing number of **Bring Your Own Devices (BYOD)**, personal laptops that users bring from home

Microsoft Intune handles AAD-joined devices very well and can also support hybrid AD/AAD setups. But for BYOD, the options become more limited. To manage a BYOD device with Intune, you usually need to enroll the device in MDM, which means pushing corporate policies (like BitLocker, Windows Hello, password rules, etc.) onto a user's personal laptop.
That's often a deal-breaker.

Why Intune Isn't Ideal for BYOD

From a user's perspective, full MDM enrollment means IT takes control of parts of the personal device. This includes enforcing password complexity, requiring disk encryption, blocking apps, and potentially wiping data. Even with "app protection policies" (MAM without enrollment), the control is limited to a few Microsoft apps like Outlook or OneDrive.
Many users, students, contractors, freelance staff, are not okay with handing over that level of control on their own hardware. Understandably so.
From an admin's point of view, managing BYOD via Intune means a trade-off: either give up control and manage nothing, or take too much control and risk pushback or non-compliance.

worXpace: Full Workspace Management, No Device Control Needed

WorXpace handles this challenge differently. It was designed to support **mixed environments** and **user-owned devices**, without requiring the device to be domain-joined or enrolled in MDM. This opens up a middle path: full workspace management *without* device-level control.
How?
On BYOD systems, worXpace uses a **voucher-based enrollment** process. The user is given a personal one-time access code (voucher), enters it during enrollment, and their device is then connected to the correct worXpace environment. It doesn't require joining the device to AAD or AD, and it doesn't apply device-wide policies like BitLocker or Hello. Instead, it focuses entirely on what the user sees and uses: apps, settings, data access, shortcuts, and environment behavior.
That means **no registry clutter, no system policies**, and **no invasive controls** on the user's laptop, just a clean, personal workspace delivered with precision.
This approach is ideal in many scenarios:

- **Students using their own laptops**: IT delivers learning tools, drives, and shortcuts without pushing BitLocker or changing local policies.
- **Contractors or temp staff**: They can get company tools for the duration of their project, with no permanent change to their device.
- **Home-office or hybrid staff**: No need to ship and manage hardware for every role; users bring their own, and worXpace delivers everything they need.

Seamless Support Across Device Types

WorXpace doesn't treat AAD, AD, and BYOD devices as separate problems. Whether the device is:

- Fully managed and domain-joined
- Azure AD joined through Intune Autopilot
- A personal laptop from home
  ...the same worXpace client can run and deliver the exact same workspace experience.

Admins can see the status of all devices, even unmanaged ones, from the central dashboard. They can push apps and workspace tasks to BYOD machines just like managed ones, all without pushing device-wide restrictions. And, just as important; the Admin can revoke the voucher and decommission the worXpace agent and remove things from the device if necessary.

No Compromises on Experience

The key strength here is that **users still get a full, rich workspace**, even on their own machines:

- They see assigned apps appear on the desktop or start menu
- They get drive mappings, printers, and config settings based on their role
- They can use **Service Point** to install extra tools or remove unneeded ones
- Everything behaves the same, whether on a corporate laptop or personal one running Windows.

And IT doesn't need to wrestle with conditional access or inconsistent device states to make this happen.

Balanced Security and Privacy

Of course, this flexibility also means worXpace doesn't enforce device security policies like Intune does, and that's intentional. The whole point is to **leave the device alone** and manage only the workspace. You give the user tools, not rules.
In environments where device security is critical, such as finance or healthcare, you can still use Intune to manage company-owned endpoints. But for students, contractors, or edge users, where you don't own the hardware, worXpace gives you a powerful and respectful way to provide everything they need without overstepping.

Complementary, Not Competing

It's important to emphasize that **Microsoft Intune and worXpace are not competitors, they complement each other** in an integrated environment. Intune continues to do what it does best: device enrollment, Windows policy enforcement, compliance checks, patch management, and conditional access enforcement. WorXpace seamlessly integrates on those same devices to handle the user space: delivering applications and settings in a granular way, providing a great user experience, and responding instantly to changes or user requests.
Many organizations use Intune as the deployment vehicle for worXpace itself. For example, you can enroll devices in Intune (via Autopilot) and as part of that onboarding, deploy the worXpace client agent through Intune (since it's just a small MSI). The worXpace agent will then automatically register with the worXpace cloud service (with Active Directory- or Azure AD joined computers it

knows which tenant it belongs to without complex configuration, on BYOD devices it invokes the voucher enrollment procedure). In this model, Intune lays the groundwork by ensuring the device is healthy and compliant, and worXpace takes over to fine-tune the workspace. They operate in concert: Intune might mandate a device encryption policy, while worXpace delivers the user's needed apps and preferences. There's no overlap that would cause conflict, each handles different layers of management.

From a CIO/CTO perspective, this combination means **maximizing the value of your Microsoft 365 investment** (Intune) while plugging its gaps with a specialized solution (worXpace) rather than seeking a wholesale replacement. WorXpace doesn't require replacing Intune's MDM; instead, it leverages Intune where appropriate and adds its own cloud service for workspace management. The learning curve for admins is also reasonable, worXpace's *management console* is designed for IT pros and uses concepts familiar to those who have managed group policies or used tools like VMware Workspace ONE or Citrix in the past. But unlike some of those older solutions, worXpace is cloud-native and aligns well with an Intune-managed modern desktop.
In summary, **Intune + worXpace together provide a complete management solution**: Intune secures and provisions devices, and worXpace delivers a flexible, user-centric workspace on those devices. The result is a secure, compliant, but also highly adaptable and user-friendly environment.

Conclusion: A Complete Solution for IT and Users

In conclusion, integrating worXpace into an Intune-managed environment empowers IT teams to deliver a far more flexible and responsive workspace without sacrificing the security and control Intune provides. **Intune** establishes a solid foundation, it ensures every device is secure, compliant, and provisioned with the basics. **WorXpace** builds on that foundation to introduce agility, rich application support, offline reliability, and a user-centric approach that modern enterprises need. The two systems work in harmony: Intune keeps the device in check, and worXpace keeps the user happy.

By adopting worXpace alongside Intune, organizations can address the common pain points (unpredictable updates, rigid app delivery, lack of customization) with a solution specifically designed to fill those gaps. The result is less frustration for IT administrators (since they can now push changes instantly, deliver any app easily, and offload routine requests to self-service) and a better experience for end-users (who gain choice, autonomy, immediate access to resources, Their BYOD device remains 'untouched'). There are no buzzwords here, just practical, observable benefits: faster rollouts, fewer helpdesk tickets, more efficient use of bandwidth (by not pushing software nobody uses), and higher productivity across the board.

For CIOs and CTOs, the Intune + worXpace approach means you don't have to abandon your investment in Microsoft's ecosystem to get advanced workspace management. WorXpace complements Intune rather than competing with it. This also means **adoption can be incremental**, you can start by using worXpace for a specific need (say, delivering an app that Intune couldn't handle well, or providing a self-service catalog for a subset of users) and expand as you see the results (and come to the conclusion that probably all applications should be handled by worXpace), all while Intune continues to manage the baseline. The learning and deployment curve is gentle, since worXpace's cloud service integrates with Active Directory and Azure AD and requires minimal setup on endpoints (no complex on-prem infrastructure to maintain).

In a world where hybrid work is the norm and user expectations are higher than ever, combining Intune's robust device management with worXpace's agile workspace management is a strategy that delivers on both IT governance and user satisfaction. It allows IT to say "yes" more often, yes, we can get you that app now; yes, you can choose how you work, without losing control or security oversight.

In summary, Intune + worXpace = a secure, dynamic, and user-friendly workspace. By combining the strengths of both, IT administrators can ensure that devices are not only compliant and secure, but also configured in the most effective way for each user. This powerful combination helps IT teams move from just managing devices to truly empowering users, all while maintaining the strong security posture that organizations demand.