Microsoft

Microsoft 365

Blog home
/ Intune

Search the blog

Engaged developer in focused work in the context of automation in manufacturing to build intelligent apps powered by Azure

Customer stories Intune Enterprise **6 min read**

Best practices in moving to cloud native endpoint management

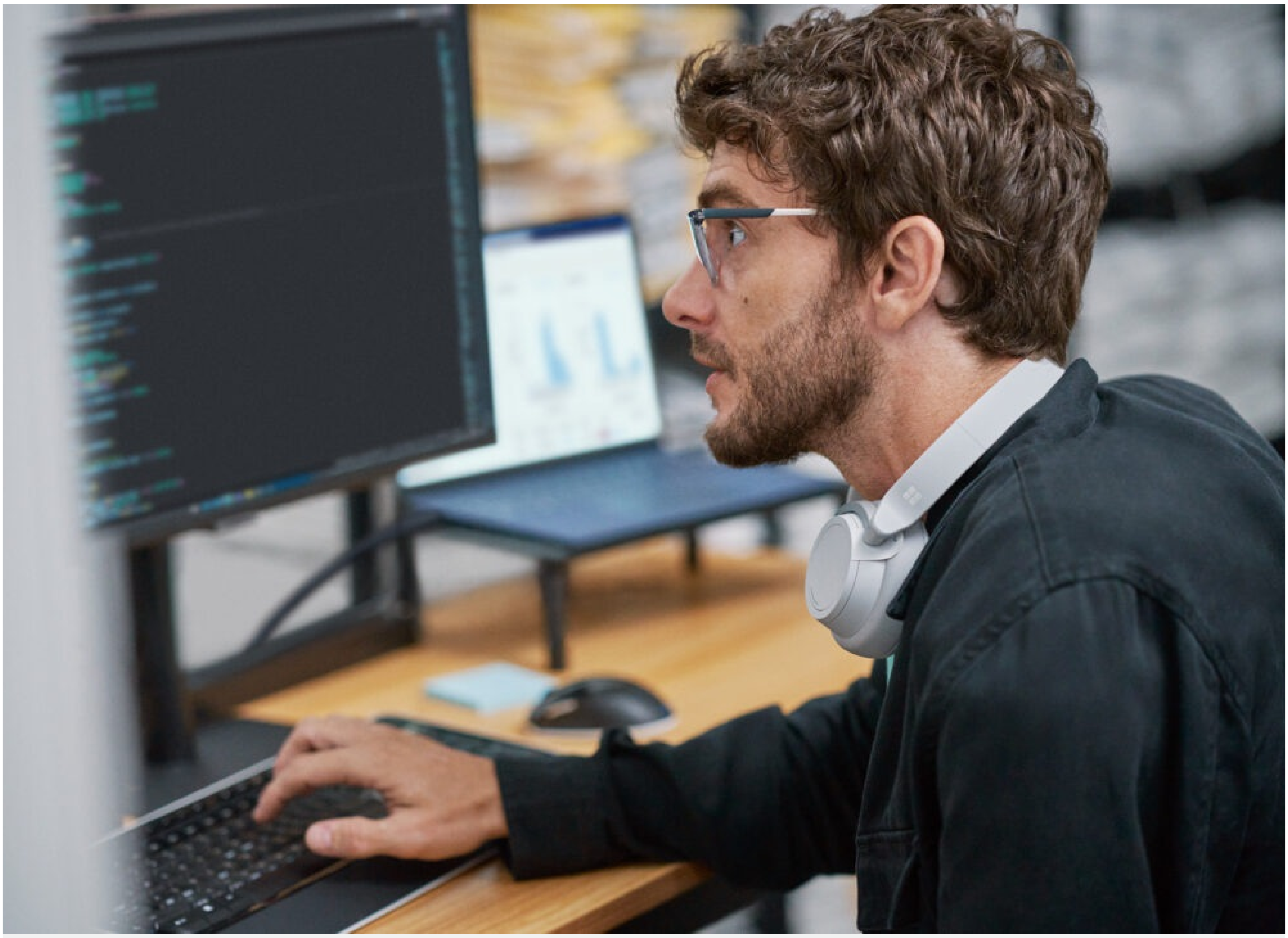
By Jason Roszak, Chief Product Officer, Microsoft Intune

January 29, 2024

Microsoft 365
Windows
Windows 11

This blog is the second of three that details our recommendation to adopt cloud native device management. In the first post, we shared three stories explaining *why* large organizations moved to a cloud-native management stance. A common thread through the customer stories was how they achieved greater security, cost savings, and readiness for the future through their cloud transformations. These benefits have been reflected in the accelerated adoption of cloud-only management we've seen from customers, and our increased investment in cloud-native scenarios in Microsoft Intune.

In this blog, I will focus on *how* you can accelerate your transition to cloud native endpoint management. Many of my customer conversations are centered on how best to transition, with the value of a cloud first approach already understood. In many cases, there is a strong desire to move to the cloud, but lack of a step-by-step plan to make the move a reality. I detail below a three-phase approach that simplifies the process of getting to fully cloud-based management. First, modernize all management workloads by moving them from on premises to Intune. Second, hybrid Entra join and enroll your existing PCs in Intune. Third, for new Windows devices, go straight to cloud native.



This three-phase approach enables you to achieve faster time to value, lessen the experience impact to your users, and finally, simplify your architecture and reduce your total cost of ownership.

Enabling workloads in Intune

Enabling all management workloads from the cloud is the fastest way to reduce the complexity and cost of current technology and get closer to a single pane of glass. When making the transition from Microsoft Configuration Manager (ConfigMgr) to Intune, there are two types of cloud workloads you will enable. The first are management functions that you move from ConfigMgr to the cloud, such as updates, app deployment, and policy configuration. The second functions are net new capabilities only made possible by the cloud—such as automation, analytics, and generative AI related workloads.

Customers often ask me whether there is a logical order for moving workloads. Given the benefits, all workloads should be moved as soon as you are able, but moving them step-by-step can make sense to align with business goals. In general, you should start by enabling the net new cloud workloads discussed above, then move the existing workloads from ConfigMgr.

For those existing workloads, a common approach is to start with compliance and security workloads, followed by policy. This helps with Zero Trust initiatives, and ensures you have strong security policies in place during the transition.

For example, Petrobras, the Brazilian energy company that moved to a cloud-native strategy with Intune, saw better policy enforcement for remote devices.

> *"Despite the increased access by our remote workforce, our recent audits have quite surprisingly revealed that we haven't had any security incidents or data leakage."*
>
> —Alexandre Ribeiro Dantas, Information Security Manager at Petrobras

With security policies in place, we often see customers next move updates (patch) workloads to the cloud to take advantage of the Microsoft modern approach to updating devices on any network, anywhere in the world. National Australia Bank (NAB) is a great example of this. Their goal was to adopt a modern approach to patching.

> *"Windows 10 was the catalyst for retooling our environment and getting to where we are today, moving patch compliance from 60% to 97% across 45,000 endpoints."*
>
> —Andrew Zahradka, Head of Workplace Compute Technology at National Australia Bank

Apps are often the last workload migrated, as there is frequently an advantage to rationalizing application estates before migrating them. When migrating apps, we don't recommend migrating all apps like-for-like from on-premises to the cloud. Instead, we recommend reviewing the apps and removing unused applications prior to migration. We have seen this result in organizations dropping from thousands of applications to hundreds that need to be migrated.

Of course, in some instances, there may be one or two workloads that can't immediately be moved to the cloud. Our recommendation here is not to let one or two laggard workloads stop you from gaining the rest of the benefits from moving to the cloud. Instead, try to manage all workloads natively in the cloud everywhere possible, and use ConfigMgr as a side car helper until you can modernize the laggard workloads.

Enroll existing Windows devices in Intune

The next step is to begin to enroll devices—enroll your clients managed by ConfigMgr into Intune and hybrid join them to Microsoft Entra ID (previously Azure Active Directory).

This is a transitory step, not the end game. It takes time to transition to the cloud and modernize your directory and management solutions. By taking this first step of enrollment and hybrid Entra join, you receive the benefits of the cloud workloads and can transition away from dual management—such as existing devices receiving workloads from on-premise ConfigMgr, and new devices from the cloud. For identity management, we recommend you hybrid join your existing devices with Entra ID while new devices are joined directly or natively with Entra ID. Hybrid join is the interim step, specifically for your existing Active Directory joined devices. It brings you the benefits of cloud without resetting and reprovisioning the device and disrupting the user. Hybrid devices will then age out of your environment as they are replaced with cloud-native, Entra join new devices through the natural lifecycle at refresh, or opportunistically if there's an event, such as break-fix, that requires a device be reimaged.

Microsoft has many partners with deep expertise in migrating Windows to the cloud who have seen success using this approach. They recently held a discussion on some of the lessons they've learned in cloud migrations, which I would encourage you to view.

Peter Klapwijk, an Infrastructure Engineer, best sums up this stage.

> *"If a company has the Intune licenses, they should definitely start switching on co-management, to make use of the benefits [of which a single portal, remote actions, and endpoint analytics were mentioned]"*
>
> —Peter Klapwijk, Infrastructure Engineer at NN Group

With new Windows deployments, go direct to cloud native

As you refresh or reset Windows devices, our recommendation is to manage them as fully cloud native. This represents an opportunity to reimagine what Windows management should look like in your organization. This greenfield approach sets a North Star for your organization's transition and reduces the risk of recreating outdated legacy approaches in the cloud.

This is especially true for Windows 11 devices. As the best version of Windows, it makes sense to use Windows 11 for any new devices, regardless of the provisioning method.

> *"Windows 11 Enterprise with Microsoft Intune has streamlined device provisioning, updates, security configurations, and troubleshooting processes. By centralizing these tasks, we've been able to achieve operational efficiencies, optimize resource allocation, and effectively manage our technology environment with a lean IT team."*
>
> —Blake T. Lunsford, Director of IT, Alabama Appellate Court System

Many customers opt to skip the co-management phase of migration completely, bringing new devices on as cloud native. These customers use their hardware refresh cycle as the catalyst to move to cloud native. Existing devices remain with on-premises management while new devices are deployed as fully cloud native. After a full hardware refresh cycle over 2-3 years, all Windows devices will eventually be managed exclusively in the cloud. For example, Cognizant empowers all its employees to implement new device setup remotely without any intervention from IT.

> *"Day one productivity was never the plan. This was a big project that was supposed to be completed over a two-year period. Yet, within a week, we started delivering a successful Autopilot Intune migration. From then on, we delivered laptops from our suppliers directly to employees at home."*
>
> —Ramesh Gopalakrishnan, Cognizant's Director for Digital Workplace Services

Lastly, customers have asked whether they should delay their Windows 11 upgrades if they are not ready to move ahead with management modernization. The guidance here is clear: prioritize rolling out Windows 11 with the management tools and processes you already have in place today, such as ConfigMgr. Or if you have non-Windows 11 capable devices but would like to leverage Windows 11 features and capabilities, you can do so with Windows 365 Cloud PC, until new capable devices have been acquired.

Next steps

We are excited to be seeing more and more companies move to a fully cloud native approach for endpoint management, so I hope if you're not there already, this blog helps you identify the proper steps to get there. No matter where you are on the journey, we encourage you to learn more and get your plans set in 2024! Keep a look out for our third and final blog in this series, where I will focus on the process of implementation and communication with stakeholders.

In the meantime, learn more about Microsoft Intune.

Connect with us on social

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads