nerdio | manager for enterprise

EDITION 2026

MICROLEARNING

Windows 365 for Agents

and the trusted runtime your AI workforce needs

By **Bas van Kaam**

PRINCIPAL LEARNER ARCHITECT

STEP 1 · WHY THIS LESSON

Today, most agents run on *ad-hoc infrastructure*. They need the same trust model as your humans.

01 Ad-hoc infrastructure today

Microsoft's own framing: many agents run on local machines, shared VMs or unmanaged cloud, creating gaps in identity, policy enforcement, auditability and control.

02 Audit logs can't tell agent from human

When an AI agent uses a human's credentials to act, audit logs cannot tell the two apart. Compliance teams flag that. So do auditors. So does Conditional Access.

03 Same trust model, extended to agents

Windows 365 for Agents puts every agent on its own Intune-managed, Entra-secured Cloud PC, with its own cryptographic identity. The trust model your employees already run on.

STEP 2 · WHAT IT IS

A new class of Cloud PC, built for digital workers.

*Windows 365 for Agents is a brand-new class of Cloud PC, built on the **same Windows 365 platform** that powers Enterprise and Business. Same Azure VM stack, same Intune, same Microsoft Entra ID. The difference: agents draw from **shared pools** through a check-out/check-in model rather than fixed user assignments.*

WINDOWS 365 FOR AGENTS AT A GLANCE

Status	Public Preview, US-only at announcement (May 1, 2026). Released alongside Agent 365 GA on the same day.
Pricing	Pay-as-you-go: USD 0.40 per VM per hour, billed per task and rounded up. 50 free hours per tenant for trial of published autonomous agents.
Prerequisites	Agent 365 license (USD 15/user/month standalone, or bundled in Microsoft 365 E7) plus Intune license plus an active Azure subscription.
Architecture	Windows 11 Enterprise 24H2 (Linux for Researcher), Microsoft Hosted Network, Entra-joined and Intune-enrolled. Stateless reset after each session.
Limits	Up to 5 Cloud PC pools per environment, 10 Cloud PCs per pool. Trial: 2 pools per tenant.

STEP 3 · TWO LAYERS, ONE WORKFORCE

Microsoft delivers the Cloud PC. Nerdio runs the workforce.

Microsoft layer is GA · Nerdio layer **on the roadmap**, *announced at NerdioCon 2026*

● MICROSOFT · IDENTITY

Microsoft Entra Agent ID

Each agent gets its own first-class identity in Entra. Not a service account, not a shared user, not a borrowed human credential.

Cryptographic, passwordless

Authentication is token-based with cryptographic credentials. Nothing to phish, nothing to leak in a screenshot, nothing to rotate by hand.

Audit-distinct from humans

Sign-in logs, Defender events and Purview activity all attribute the agent identity separately from the human who delegated the work.

● MICROSOFT · POOLS

Warm or cold Cloud PC pools

Warm pools are pre-provisioned for fast checkout. Cold pools spin up on demand for lower idle cost. Each pool is policy-governed.

Check-out, run, check-in

An agent reserves a Cloud PC for one task, performs the work, then releases it back to the pool. The same VM serves the next caller.

Stateless reset every session

Cloud PCs reset after every agent session, with no state carried forward. Nothing to leak between agents, nothing to clean up by hand.

● NERDIO · WORKFORCE

One platform for users and agents

Manage humans and digital workers side by side in Nerdio Manager, instead of juggling two consoles for two kinds of workforce.

Provisioning parity

Agent provisioning policies sit beside user policies in the same UI, with the same image, app and Intune controls applied.

Lifecycle visibility across both

Same lifecycle view across user Cloud PCs and agent Cloud PCs: provisioned, in-use, idle, retired. One operational picture, not two.

● NERDIO · COST

Agent compute in cost dashboards

Pay-as-you-go agent hours land in the same cost analysis views as user Cloud PCs and AVD, so finance sees one budget across both.

Warm pool capacity insights

Capacity reports show whether warm pools are right-sized for peak agent demand or quietly burning idle hours overnight.

Unified observability

Session logs, errors and runtime patterns aggregated across all agent pools, ready to feed back into the policies that govern them.

STEP 4 · HOW IT WORKS

From "agent has work to do" to "billed, audited, returned to pool" in five moves

0

Confirm the three prerequisites ONE-OFF

An **Agent 365 license** (USD 15/user/month standalone, or bundled in Microsoft 365 E7), an **Intune license** and an **active Azure subscription**. Public Preview is currently US-only.

1

Create the provisioning policy (agents)

In the `Microsoft Intune admin centre`, create a **provisioning policy (agents)**. Policy-based, not device-based: it groups Cloud PCs by team or workload.

2

Configure the pool: warm or cold

Choose **warm** for pre-provisioned, fast-checkout capacity, or **cold** for on-demand spin-up with lower idle cost. Set the pool size within Public Preview limits.

3

Register the agent in Agent 365

Each agent receives its own **Microsoft Entra Agent ID**: cryptographic, passwordless, audit-distinct from human users. Permissions are explicitly scoped per agent.

4

Agent checks out, runs, checks in

The agent reserves a Cloud PC, performs its task, returns it to the pool. Compute is billed per VM per hour. Reset triggers automatically. Next caller gets a clean VM.

STEP 5 · THE INSIGHT TO REMEMBER

A Cloud PC for Agents is not a different Windows.

*It is **the same Windows 365**, with an identity model and a lifecycle built for digital workers instead of humans.*

STEP 6 · IN PRACTICE

The 18-supplier-portals scenario

TODAY

A 320-employee distribution company sources from 18 supplier portals, none of which expose APIs. Every morning, three procurement coordinators spend 90 minutes each typing yesterday's prices into spreadsheets. The work is mechanical, error-prone and impossible to audit cleanly. The company already runs Microsoft 365 E5, Intune and Conditional Access for its human users.

18	3	90 min	0
SUPPLIER PORTALS	COORDINATORS	EACH, PER DAY	AUDIT TRAIL

WITH WINDOWS 365 FOR AGENTS

A Copilot Studio agent with its own Microsoft Entra Agent ID checks out a Cloud PC from a warm pool each morning, navigates all 18 portals through the UI, saves a clean CSV to SharePoint, then checks the Cloud PC back in. The audit log shows the agent did the work, not "Sjoerd from procurement". When Nerdio Manager support lands, the agent pool sits next to the user Cloud PCs in one console.

✓ **Own Entra identity**
Agent acts as itself, not as a borrowed human

✓ **Stateless Cloud PC**
Reset after every run, nothing leaks between sessions

✓ **Pay only per task**
~0.6 hour × USD 0.40 = USD 0.24 per run

270 min/day of repetitive portal work moved to a digital worker · clean audit trail per run · coordinators redeployed to supplier negotiation

STEP 7 · NOW YOU TRY

Three questions to lock the lesson in

Q · 01

Why is "agents borrowing human credentials" an audit and Conditional Access problem, not just an etiquette one?

Hint: *Audit logs can't tell the two apart. Conditional Access can't either. Both treat the agent as the human.*

Q · 02

Which two architectural pieces together stop an agent from doing more than it was designed to?

Hint: *Stateless reset of the Cloud PC after every session, plus the agent's own Entra identity with explicitly scoped permissions.*

Q · 03

In your environment, which task today is repetitive, UI-bound and screams "give it to a digital worker"?

Hint: *Look for portals without APIs, daily mechanical entry, and tasks where the audit trail is currently a screenshot.*

TAKE-AWAY

Same Cloud PC. Same Intune. Same Entra.
The desktop just **belongs to a digital worker now**.

Found this useful? Share it with one colleague preparing IT for the agent workforce.

BAS VAN KAAM · PRINCIPAL LEARNER ARCHITECT AT NERDIO