CTO Sunday Thoughts #14

MyPlatform

AI needs secure infrastructure

AI is no longer a side-project - It is becoming infrastructure.

At Microsoft Ignite 2025, one message stood out clearly beneath all the product launches and demos: AI is moving from experiments to **operating model**. Agent 365. Work IQ. Fabric IQ. Foundry IQ. The era of agentic systems running across the enterprise has officially begun.

But here is the uncomfortable truth:

You cannot scale intelligence on top of an ungoverned platform.

From features to foundations

For years, organizations have added cloud features at speed. More services. More data. More integrations. Now we are about to add **autonomous AI agents** into that already complex environment.

Agents that can:

- Read enterprise data.
- Act on business systems.
- Trigger workflows.
- Make decisions at machine speed.

This changes everything.

Because when an agent fails, leaks data, or makes a wrong decision, the root cause will almost always sit **below** the agent - in identity, policy, access, logging, and governance.

AI does not remove the need for infrastructure. It **amplifies** it.

The new intelligence stack

Ignite introduced a new logical stack for AI-driven enterprises:

Work IQ - the work and collaboration context from Microsoft 365.

Fabric IQ - the semantic business data layer.

Foundry IQ - the knowledge, retrieval, and grounding layer.

Agent 365 - the agent lifecycle and control plane.

This is powerful. It gives agents memory, business context, knowledge, and execution capabilities.

But it also creates a new reality:

Every agent becomes a privileged digital worker.

- It has identity.
- It has access.
- It consumes sensitive data.
- It triggers actions in production systems.

Which means that every agent must be governed like production infrastructure.

The real risk is not the model

Most conversations about AI risk still focus on the model: hallucinations, accuracy, bias.

Those matter.

But in real enterprises, the biggest risks will come from:

- Uncontrolled **agent sprawl**
- Weak or inherited **identity and RBAC**
- Over-exposed **data through semantic layers**
- Missing **logging and audit trails**
- No defined **agent lifecycle governance**
- Compliance teams seeing agents only *after* they are already in production

This is not an AI problem.

This is an **infrastructure and governance problem**.

The blueprint for governed AI

If AI is infrastructure, then it must be treated like infrastructure from day one:

1. **Tenant-first, identity-first**
   Agents must live inside the customer tenant, bound to Entra identities, not floating around as external black boxes.
2. **CAF-aligned Azure foundation**
   Management groups, policies, networking, security baselines, logging. Before agents. Not after.
3. **Governed data semantics**
   Fabric IQ is powerful, but semantic models without access control become a data leakage engine.
4. **Controlled knowledge retrieval**
   Foundry IQ must respect classification, sensitivity, and regulatory boundaries.
5. **Agent lifecycle as a controlled process**
   POC → Pilot → Production must be gated by policy, not enthusiasm.

6. **Evergreen compliance**
   As Microsoft changes the control plane, governance must adapt automatically. Not through new projects.

This is exactly where we see the next bottleneck forming for enterprises.

Not in building agents.

But in **operating them safely, at scale, over time.**

The strategic shift for leadership

For CTOs, CISOs, CIOs and boards, the question is no longer:

“How fast can we build AI?”

The real question is:

“How fast can we govern what we deploy?”

Because in the next phase of digital transformation, the most dangerous organizations will not be the slow ones.

They will be the fast ones **without foundations**.

The vision

AI-driven business with confidence.

Scale without losing control.

Innovation without compliance debt.

Autonomy without chaos.

That future does not start with better prompts.

It starts with **secure infrastructure**.

And this time, the foundation truly decides the outcome - This is MyPlatform