MICROSOFT AGENT 365 · AGENT GOVERNANCE & SECURITY

Agent 365, activated with discipline

Sequenced enablement across Entra ID, Purview, and Defender.

/ The problem

The agents are already in your tenant. Agent 365 is the control plane built to govern them — but most of its value is **Purview, Defender, and Entra ID working underneath**. Switched on without an operating model, it produces alerts no one triages and inventory no one curates.

What Agent 365 does — and what it depends on

Inventory the estate
Microsoft, partner, multi-cloud, and shadow agents — one registry.

Identity through Entra ID
Agents inherit user permissions; your file structure is the AI access model.

Guardrails through Purview
DLP and label-based control work only when labels actually exist.

Detection through Defender
Shadow-agent discovery and runtime blocking — if someone owns the queue.

Evidence you can attest to
Interaction logging at regulator-grade recordkeeping standard.

Activation without an operating model is the problem.
Sequenced enablement is the path.

Identient pairs Agent 365 activation with the ownership, policy, training, and reporting that make it hold.

/ How we engage

1

DIAGNOSE

Agent estate assessment

Inventory agents, scan identity exposure, assess Purview readiness and licensing cost-to-value.

2

DESIGN

Operating model

Risk tiers mapped to Purview's taxonomy; AIRB with a named triage owner; use standard signed off.

3

DEPLOY

Sequenced activation

Inventory first, then policy enforcement, then reporting — operators trained before switches flip.

4

DEFEND

Governance that holds

Monthly AIRB metrics, drift checks, continuous attestation.

*Accelerated by the **Hybrid Twin** — an AI GRC agent grounded in your policies, answering your team in Teams or Slack.*

Where the work actually is

Entra ID & identity

Agents inherit user permissions, so **SharePoint and OneDrive hygiene is upstream of every agent control**. We map least-privilege access, close stale sharing, and finish the identity groundwork first.

Purview, operationalized

An unused Purview license is **governance left on the shelf**. We take classification from paper into operation: labels mapped to your risk tiers, DLP authored and tuned.

Defender, with an owner

Detection reduces risk only when **someone owns the queue**. We name and train the owner, stand up triage with SLAs, and wire findings into AIRB reporting.

Why Identient

- **Operator-led**
  Founder-led by an operator who has run identity and security at scale — VMware, Oracle, PwC, Optiv.
- **Identity-first**
  Every AI control inherits its strength from identity — our deepest practice.
- **A framework, not improvisation**
  Four phases, five control dimensions. Verification Debt descends; discipline remains.
- **Honest about timing**
  We put licensing cost-to-value on the table — and will tell you when activation should wait.

Proof, not promises: **from zero AI governance to an operating AI Review Board and governed agents in daily use — in one quarter**, at a FINRA-regulated financial services firm.

Fintech
FINRA-grade recordkeeping · SOC 2 cycles

Healthcare
HIPAA audit · FDA SaMD evidence

High Tech & SaaS
IP protection · security-questionnaire scrutiny

Begin where you are

Most engagements begin with a four-to-six-week Diagnose, sized to your agent footprint and regulatory context — then run as an integrated program or discrete modules.

Steve Tout
CEO, Identient Corp.
steve@identient.ai · identient.com