AGENT 365 FOUNDATIONS: 6-WEEK DISCOVERY & SECURITY SETUP

REPLY

This engagement provides a focused, six-week programme to help organisations understand their current agent landscape, regain control over fragmented or unmanaged AI activity, and establish a secure, compliant baseline using Microsoft Agent 365, Entra Agent ID, Purview DLP for AI, and Defender for AI. The aim is to produce clear visibility of all agents operating across the enterprise, implement essential identity and data protection controls, and define the roadmap for more advanced engineering such as MCP servers, SDK-based integrations, and an AI Centre of Excellence.

STAGED APPROACH

Stage 1 – Discovery & Readiness (Weeks 1–3)
The engagement begins with mobilization, establishing access, validating prerequisites, and aligning on business objectives, regulatory obligations, and the organization's risk posture.

Stage 2 – Governance & Security Foundations (Weeks 4–6)
The second stage focuses on implementing the essential controls that allow enterprises to operate autonomous agents safely.

OVERALL OUTCOMES TO EXPECT

By the end of the six weeks, organizations gain full visibility of their existing agent footprint, a clearly defined architecture, and formalized baseline controls spanning identity, data protection, and runtime security. They also receive the complete set of artefacts required to operate Agent 365 in a compliant and scalable manner.

THANK YOU

www.reply.com

REPLY