GOBERNANZA DE AGENTES DE IA

Sesiones de arquitectura y diseño (ADS) para Agent 365

Hay interés, pero no una arquitectura ni una hoja de ruta acordadas

El interés en los agentes es real, pero no hay una arquitectura ni una hoja de ruta acordadas. Conviven propuestas internas que compiten entre sí, sin un modelo de gobernanza objetivo definido.

Sigue sin estar claro quién aprueba un agente y con qué acceso, y no hay un plan acordado para gobernar agentes a escala.

En todo el mercado, la magnitud de esa brecha ya es medible:

PUNTOS CIEGOS

82%

... descubrió agentes desconocidos en el último año

Cloud Security Alliance & Zenity, 2026 (n=445)

INFILTRACIÓN DE ACCESO

53%

... ha tenido agentes que exceden los permisos previstos

Cloud Security Alliance & Zenity, 2026 (n=445)

BRECHA DE POLÍTICA

31%

... ha adoptado formalmente una política de agentes

Cloud Security Alliance & Zenity, 2026 (n=445)

Antes de construir, el diseño debe estar acordado.

Eso es lo que aporta nuestra experiencia E-nvision: casos de uso predefinidos de alto impacto, con la profundidad que necesitan sus equipos.

Presentamos Agent 365 E-nvision de Synergy Advisors

E-nvision es la Architectural Design Session (ADS) de Synergy Advisors creada para este momento: hasta tres casos de uso predefinidos de alto impacto, basados en nuestra experiencia, discutidos en profundidad con un experto y validados como un diseño de alto nivel en un entorno funcional.

Existe porque las decisiones de gobernanza que se toman tras el despliegue son las costosas. Diseñado para patrocinadores, arquitectos y responsables de carga de trabajo, en nivel 300/400, y entregado en remoto y uno a uno – la siguiente página detalla cómo se desarrollan las sesiones.

- Escenarios y arquitectura de alto nivel validados en un entorno funcional, sin cambios en sus entornos.
- Hasta tres casos de uso predefinidos de alto impacto, discutidos en profundidad con un experto.
- Las consideraciones de gobernanza se resuelven antes de que comience la implementación.
- El patrocinador, los arquitectos y los propietarios de la carga de trabajo, alineados en un diseño que todos comparten.

Agent 365 (A365) – Casos de uso de alto impacto predefinidos

NÚCLEO

Observar los agentes y prevenir su proliferación
Inventario unificado de agentes en todas las plataformas, que identifica los que no tienen responsable o están en riesgo

Incorporar agentes con acceso de mínimo privilegio
Plantillas de aprobación, paquetes de acceso de Entra, validación del patrocinador y acceso condicional

Gobernar las herramientas de los agentes MEJORADO
Control de las herramientas que usan los agentes en apps como Outlook y SharePoint, con cada acción auditada

Evitar la sobreexposición de datos y sus riesgos
Purview DSPM para IA, DLP y Communication Compliance sobre el acceso de los agentes a datos sensibles

Defenderse de amenazas y vulnerabilidades de IA
Investigación de inyecciones de prompts, contención de agentes comprometidos y búsqueda en herramientas MCP

Auditoría, cumplimiento y ciclo de vida del agente
Exportación del registro de auditoría, bloqueo o eliminación de agentes no conformes y retención de registros

Descubrir y controlar agentes de IA locales NUEVO
Detección de extensiones de IDE, CLI y editores de código que actúan como agentes locales en dispositivos administrados, y bloqueo con Intune de los no aprobados

BETTER TOGETHER

Agent 365 + Defender for Endpoint
Detección e investigación de agentes en endpoints

Agent 365 + Microsoft Sentinel
Detección, búsqueda de amenazas y respuesta a incidentes

Agent 365 + Defender for Cloud
Riesgos en los datos de grounding y rutas de ataque

Agent 365 + Azure API Management NUEVO
Gateway de IA para modelos, servidores MCP y herramientas

AGENT 365 SDK

LangChain
Gobernado desde Agent 365 durante todo su ciclo de vida

LangGraph
Incorporado con el SDK, con la misma observabilidad y controles

Google ADK
Registrado con el SDK: identidad, propietario y observabilidad

Amazon Bedrock AgentCore NUEVO
Plataforma conectada e integración profunda con el SDK

Más plataformas de agentes PRÓXIMAMENTE
Microsoft Agent Framework, OpenAI, Anthropic, Salesforce, SAP, Kubernetes

Experiencias de E-nvision (Sesiones de arquitectura y diseño)

VÍA DE INFRAESTRUCTURA

Hasta **4** SESIONES — Hasta **2** POR SESIÓN

Vía de Infraestructura

- ✓ Hasta tres casos de uso (incluido el descubrimiento), discutidos con un experto en un entorno funcional
- ✓ Escenarios, consideraciones de arquitectura y gobernanza validados de forma interactiva
- ✓ Requisitos y diseño de alto nivel del caso de uso, validado, en Nivel 300

VÍA DE DESARROLLO

Hasta **4** SESIONES — Hasta **2** POR SESIÓN

Vía de Desarrollo

- ✓ Hasta tres casos de uso (incluido el descubrimiento), centrados en escenarios de agentes de terceros con el SDK Agent 365
- ✓ Integración, propiedad y diseño del ciclo de vida con SDK para agentes externos
- ✓ Requisitos y diseño de alto nivel del caso de uso, validado, en Nivel 400

Alcance y entregables

Vía de Infraestructura

EN ALCANCE

- ✓ Hasta 3 casos de uso predefinidos de alto impacto, basados en la experiencia de Synergy Advisors
- ✓ Validación de escenarios en un entorno funcional
- ✓ Gobernanza y alineación operativa
- ✓ Arquitectura de alto nivel revisada con un experto

FUERA DE ALCANCE

- ✕ Cambios en entornos de producción o pruebas
- ✕ Tareas de desarrollo o despliegue personalizadas

ENTREGABLES

- ● Diseño de alto nivel del caso de uso validado
- ● Resumen de validación de arquitectura
- ● Gobernanza y recomendaciones para el siguiente paso

Vía de Desarrollo

EN ALCANCE

- ✓ Hasta 3 casos de uso en escenarios de agentes de terceros
- ✓ Arquitectura diseñada con el SDK Agent 365
- ✓ Integración, propiedad y diseño del ciclo de vida
- ✓ Arquitectura de alto nivel revisada con un experto

FUERA DE ALCANCE

- ✕ Cambios en entornos de producción o pruebas
- ✕ Tecnologías fuera de los objetivos del taller

ENTREGABLES

- ● Diseño de alto nivel del caso de uso validado
- ● Resumen de validación de arquitectura
- ● Gobernanza y recomendaciones para el siguiente paso

AGENT 365 SDK · AGENTES DE TERCEROS

Agent 365 más allá de Microsoft

Agentes de AWS, Google Cloud, LangChain y LangGraph, gobernados en el mismo plano de control de Agent 365 que Copilot. Nuestros expertos validan y extienden lo que Agent 365 cubre de forma nativa, para que cada agente cumpla cinco condiciones.

PLATAFORMA	DESCUBRIMIENTO	IDENTIDAD	PROTECCIÓN DE SEGURIDAD	PROTECCIÓN DE DATOS	TELEMETRÍA
Amazon Bedrock AgentCore AWS	Nativo	No cubierto	Parcial	No cubierto	Parcial
Google ADK Gemini Enterprise Agent Platform	Nativo	No cubierto	Parcial	No cubierto	Parcial
LangChain Framework de agentes	No cubierto	No cubierto	No cubierto	No cubierto	No cubierto
LangGraph Framework de agentes	No cubierto	No cubierto	No cubierto	No cubierto	No cubierto
Con el Agent 365 SDK Ya implementado por Synergy Advisors Entra Agent ID · Purview · OpenTelemetry	Integrado	Integrado	Integrado	Integrado	Integrado

Nativo — Cubierto de forma nativa mediante plataformas conectadas

Parcial — Solo señales de lectura, sin controles en el código

No cubierto — Requiere integración en el código con el Agent 365 SDK

Integrado — Integrado con el Agent 365 SDK

Fuente: Synergy Advisors, portafolio Agent 365 E-xperiences V.1.8 (diapositiva 48); Microsoft Learn, Connected platforms in Agent 365.

De forma nativa y extendido con el Agent 365 SDK

Descubrimiento	Cada agente registrado en Agent 365, con un responsable y un patrocinador.
Identidad	Su propio Microsoft Entra Agent ID y acceso condicional basado en riesgo.
Protección de seguridad	Advanced Hunting de Defender y Microsoft Sentinel, una sola respuesta del SOC.
Protección de datos	Purview DLP evalúa cada prompt y respuesta en tiempo real.
Telemetría	Quién usa cada agente, con qué frecuencia y cuánto, con OpenTelemetry.

En AWS y Google Cloud: de la visibilidad al control

Los agentes se quedan donde se ejecutan. En Google Cloud, los callbacks de ADK envían los prompts a Purview.

NIVEL 1

Visibilidad conectada

- ✓ El agente aparece en Agent 365
- ✓ Actividad sincronizada desde Amazon CloudWatch
- ✓ Operaciones en Advanced Hunting de Defender

NIVEL 2

Integración profunda

- ✓ DLP de Purview en tiempo real en cada prompt
- ✓ Contenido sensible bloqueado
- ✓ Evidencia de DLP en el Explorador de actividad

Nuevo · E-mmersion Dev Track

Un laboratorio práctico para desarrolladores y equipos de plataforma (nivel 400): su equipo incorpora agentes de LangChain, LangGraph y Google ADK con el Agent 365 SDK, Entra Agent ID y acceso de mínimo privilegio.

Hasta 4 horas · Presencial o remoto · En inglés o español · Laboratorio preconfigurado, sin cambios en su tenant

Próximamente en el Agent 365 SDK: Microsoft Agent Framework, OpenAI Agents SDK, Anthropic Claude, Salesforce Agentforce, SAP y Kubernetes administrado. Cualquier otro agente de IA: a365@synergyadvisors.biz

Cómo se desarrollan las sesiones

01

Preparación

Objetivos, partes interesadas y agenda acordados antes del primer día.

02

Revisión del entorno

Su infraestructura revisada para detectar brechas y requisitos.

03

Casos de uso

Escenarios predefinidos asignados a objetivos estratégicos (hasta 3).

04

Visión de soluciones

Arquitectura de alto nivel validada en un entorno funcional.

05

Diseño

El diseño propuesto fue revisado y validado con sus equipos.

06

Entrega

Se entregan los requisitos y las recomendaciones de diseño y despliegue.

Un portafolio de experiencias, un recorrido de gobernanza

ALINEAR Y DISEÑAR

Generar alineación y acordar el modelo objetivo

E-nsights

E-nvision

EXPERIMENTAR

Comprobar su funcionamiento y demostrarlo en un laboratorio dedicado

E-mmersion

E-xplorer

VALIDAR Y DECIDIR

Validar la funcionalidad antes de producción

E-valuation

PILOTO Y ESCALA

Pasar a producción y ampliar la gobernanza

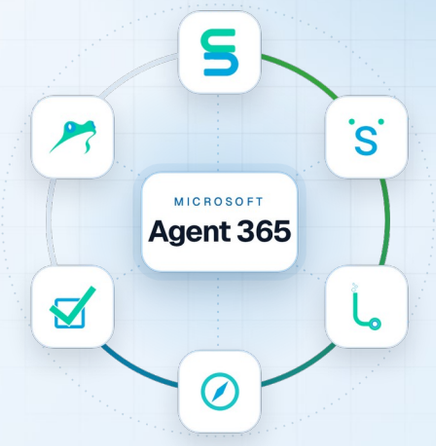
E-Scuba

Defina la gobernanza y valide el diseño

Se lleva un modelo de gobernanza objetivo acordado por sus equipos y un diseño de alto nivel validado de los casos de uso que priorizó.

Las decisiones de gobernanza se toman antes de iniciar la implementación, con el esfuerzo, la secuencia y las dependencias claros desde el principio.

Demos el siguiente paso juntos.



Para más información, no dude en contactarnos en a365@synergyadvisors.biz

Más información →