SYNERGY ADVISORS

E-xplorer

GOBERNANZA DE AGENTES DE IA

Prueba de concepto (PoC) para la gobernanza de Agent 365

Un escenario prioritario elegido, pero aún no validado

Los equipos ya eligieron un escenario prioritario, pero aún no lo validan. Los agentes desarrollados internamente requieren pruebas estructuradas en laboratorio, y la aprobación permanece bloqueada sin evidencia práctica de gobernanza.

Quienes evalúan un piloto necesitan evidencia documentada para sustentar esa decisión: constancia de lo que se configuró, se probó y se confirmó que funciona.

En el mercado, esa brecha ya es medible:

PUNTOS CIEGOS

82%

...detectaron agentes no inventariados en el último año

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

EXCESO DE ACCESOS

53%

...han tenido agentes que excedieron los permisos previstos

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

BRECHA DE POLÍTICAS

31%

...han adoptado formalmente una política de agentes

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

Antes de comprometerse, el escenario debe estar probado.

Eso es lo que entrega nuestra experiencia E-xplorer, sobre los escenarios que usted elija y con la profundidad que sus equipos requieran.

Presentamos Synergy Advisors Agent 365 E-xplorer

E-xplorer es la Prueba de concepto (PoC) que Synergy Advisors creó para este momento: un entorno Agent 365 preconfigurado y aislado, listo desde el día uno, donde los escenarios prioritarios seleccionados por usted se configuran, se ejercitan y se validan funcionalmente.

Existe porque una demostración rara vez resuelve una decisión real. Que la gobernanza funcione en el tenant de otro no equivale a que se sostenga en el suyo. Dirigido a equipos técnicos y responsables de cargas de trabajo en Nivel 300 (TDM), con entrega remota: la página siguiente detalla cómo se desarrollan las sesiones.

- Un laboratorio dedicado, solo suyo, que se explora a su propio ritmo y no en una única sesión guiada.
- Un especialista técnico a su lado, que resuelve dudas y valida su diseño conforme avanza.
- Arquitectura y funcionalidad confirmadas con evidencia, antes de tomar una decisión de adopción.
- Libertad total para probar, romper y reconfigurar cuantas veces haga falta, sin afectar su tenant de producción.

SYNERGY ADVISORS

E-xplorer

Agent 365 (A365) – Casos de uso clave

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 E-xplorer (prueba de concepto – PoC)

EXPERIENCIA BASE

Hasta **2** SEMANAS — Hasta **2** CASOS

Experiencia Base

- ✓ Acceso privado y ampliado al laboratorio hasta 2 semanas, a su propio ritmo
- ✓ Sesiones privadas con expertos para validar diseño y funcionalidad
- ✓ Hasta 2 casos de uso validados funcionalmente, no una capacitación

Alcance extendido (Plus)

Hasta **3** SEMANAS — Hasta **3** CASOS

Alcance extendido (Plus)

- ✓ La misma experiencia, extendida hasta 3 semanas
- ✓ Un tercer caso de uso, que puede incluir desarrollo
- ✓ Escenarios de agentes de terceros y Better Together incluidos

Alcance y entregables

Experiencia Base

EN ALCANCE

- ✓ Laboratorio Agent 365 preconfigurado y aislado
- ✓ Hasta 2 semanas de acceso privado ampliado
- ✓ Montaje y hasta 2 casos de uso validados
- ✓ Sesiones privadas con especialista dedicado

FUERA DE ALCANCE

- ✕ Trabajo en su tenant de producción
- ✕ Desarrollo fuera de los casos acordados

ENTREGABLES

- Validación de arquitectura y diseño
- Resumen de validación funcional
- Recomendaciones de próximos pasos

Alcance extendido (Plus)

EN ALCANCE

- ✓ Laboratorio Agent 365 preconfigurado y aislado
- ✓ Hasta 3 semanas de acceso privado ampliado
- ✓ Hasta 3 casos de uso, uno con desarrollo
- ✓ Agentes de terceros y Better Together

FUERA DE ALCANCE

- ✕ Trabajo en su tenant de producción
- ✕ Desarrollo fuera de los casos acordados

ENTREGABLES

- Validación de arquitectura y diseño
- Resumen de validación funcional
- Recomendaciones de próximos pasos

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

SYNERGY ADVISORS

E-xplorer

Cómo se desarrollan las sesiones

01

Arranque

Laboratorio preconfigurado listo desde el día uno, con casos de uso comunes acordados de antemano.

02

Visibilidad

Escenario listo: descubrimiento, inventario y exposición de IA no autorizada.

03

Protección

Escenario listo: tipos de información sensible, DLP y pruebas de uso indebido.

04

Gobernanza

Escenario listo: ciclo de vida para publicar, autorizar y retirar.

05

Evidencia

Sesiones prácticas guiadas sobre los escenarios que usted seleccione.

06

Decisión

Diseño validado y evidencia para decidir la implementación.

Un portafolio de experiencias, un mismo camino de gobernanza

ALINEAR Y DISEÑAR

Generar alineación y acordar el modelo objetivo

E-nsights

E-nvision

EXPERIMENTAR Y DEMOSTRAR

Mostrar que funciona y luego demostrarlo en un laboratorio dedicado

E-mmersion

E-xplorer

VALIDAR Y DECIDIR

Validar la funcionalidad antes de producción

E-valuation

PILOTEAR Y ESCALAR

Pasar a producción y ampliar la gobernanza

E-Scuba

Decida con evidencia, no con supuestos

Al finalizar, usted cuenta con la funcionalidad validada en los casos de uso prioritarios que seleccionó, y con la arquitectura y el diseño confirmados antes de invertir en producción.

La pregunta ya no es si esto funciona, sino hasta dónde conviene llevarlo.

Demos juntos el siguiente paso.



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

Más información →