GOBERNANZA DE IA

Laboratorio práctico guiado para la gobernanza de agentes de IA

Una evaluación técnica detenida sin prueba práctica

Ya hay proliferación de agentes y agentes sin propietario en el tenant, seguridad pregunta por sobreexposición y amenazas de IA, y falta un lugar seguro para probar gobernanza de agentes en Microsoft 365.

Las diapositivas no lo resuelven. Sus administradores necesitan tiempo real de teclado para ver cómo funciona la gobernanza, qué riesgos tiene y qué logra.

En el mercado, el tamaño de esa brecha ya es medible:

PUNTOS CIEGOS

82%

...descubrió agentes desconocidos el año pasado

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

EXCESO DE ACCESOS

53%

...tuvo agentes que exceden los permisos previstos

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

BRECHA DE POLÍTICA

31%

...adoptó formalmente una política de agentes

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

Antes de comprometerse, su equipo debe verlo funcionar.

Eso entrega nuestra experiencia E-mmersion, en los casos de uso más comunes y con un experto junto a su equipo.

Presentamos Synergy Advisors Agent 365 E-mmersion

E-mmersion es el laboratorio práctico guiado que Synergy Advisors creó para este momento: un laboratorio de Agent 365 guiado por expertos donde su equipo completa el descubrimiento y hasta 3 de los casos de uso más comunes, configurados, validados y operados en vivo.

Existe porque una demostración rara vez resuelve una decisión real. Su propio equipo configura, valida e interactúa con la tecnología. Para administradores de IA e identidad, propietarios de agentes y equipos de ciberseguridad Nivel 300 (TDM), presencial o remoto – la página siguiente detalla cómo se desarrolla el laboratorio.

- Lecciones del campo: experiencia real validando los casos de uso más comunes de Agent 365, no una demo guionizada.
- Guía experta durante todo el laboratorio, respondiendo las preguntas de su equipo en tiempo real.
- Cómo funciona la gobernanza, dónde están sus riesgos y qué logra, visto en escenarios reales.
- Corre en un laboratorio preconfigurado, sin instalación, sin riesgo y sin cambios en su tenant.

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-mmersion (laboratorio práctico guiado)

EXPERIENCIA BASE

Hasta **3h** POR SESIÓN

Hasta **3** CASOS DE USO

Experiencia Base

- ✓ Laboratorio guiado: configure, valide e interactúe directamente con la tecnología
- ✓ Descubrimiento y hasta 3 de los casos de uso más comunes, guiado por un experto
- ✓ Tiempo real de teclado para su propio equipo, no una demostración

ALCANCE EXTENDIDO (PLUS)

Hasta **8h** POR SESIÓN

Hasta **5** CASOS DE USO

Alcance extendido (Plus)

- ✓ Todo lo de la experiencia base, en un laboratorio guiado extendido
- ✓ Descubrimiento y hasta 5 de los casos de uso más comunes
- ✓ Escenarios de agentes de terceros y Better Together configurados en vivo

Alcance y entregables

Experiencia Base

EN ALCANCE

- ✓ Laboratorio guiado, hasta 3 horas
- ✓ Descubrimiento y hasta 3 casos de uso comunes
- ✓ Configuración y validación prácticas por su equipo

FUERA DE ALCANCE

- ✕ Cambios en entornos de producción o prueba
- ✕ Desarrollo a la medida

ENTREGABLES

- Informe de sesión con observaciones y recomendaciones
- Modelo operativo, aprendizajes clave y hoja de ruta

Alcance extendido (Plus)

EN ALCANCE

- ✓ Laboratorio guiado extendido, hasta 8 horas
- ✓ Descubrimiento y hasta 5 casos de uso comunes
- ✓ Escenarios de agentes de terceros y Better Together

FUERA DE ALCANCE

- ✕ Cambios en producción o desarrollo a la medida
- ✕ Acceso al laboratorio tras la sesión

ENTREGABLES

- Informe de sesión con observaciones y recomendaciones
- Modelo operativo, aprendizajes clave y hoja de ruta

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-mmersion

Cómo se desarrolla el laboratorio

01
Inicio
Agent 365 como plano de control empresarial.

02
Observar
Registro, Agent Map, inventario, dependencias y postura.

03
Gobernar
Aprobaciones, propiedad, gestión de accesos y ciclo de vida.

04
Asegurar
Sobreexposición, eventos DLP, riesgo de identidad e inyección de prompts.

05
Identificar
Casos de uso comunes y oportunidades de gobernanza.

06
Recomendar
Modelo operativo, aprendizajes clave y hoja de ruta.

Un portafolio de experiencias, un camino de gobernanza

ALINEAR Y DISEÑAR

Crear alineación y acordar el modelo objetivo

E-nsights
E-nvision

VIVIR Y PROBAR

Mostrarlo y probarlo en un laboratorio dedicado

E-mmersion
E-xplorer

VALIDAR Y DECIDIR

Validar funcionalmente antes de producción

E-valuation

PILOTO Y ESCALA

Pasar a producción y extender la gobernanza

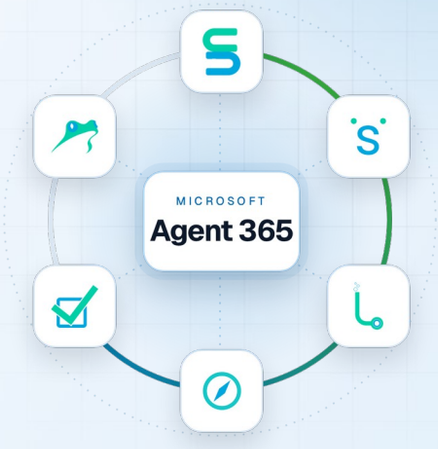
E-Scuba

Gobierne cada agente desde el primer día

E-mmersion es un laboratorio práctico: en una sesión guiada, sus administradores configuran y prueban los casos de uso más comunes de Agent 365 en un entorno seguro, con nuestros expertos.

En lugar de ver una demo, su equipo ve la gobernanza de extremo a extremo, de la incorporación a la auditoría, y aprende qué implicaría adoptarla.

Demos juntos el siguiente paso.



Para más información, contáctenos en
a365@synergyadvisors.biz

Conocer más →