SYNERGY ADVISORS

E-valuation

GOBERNANZA DE AGENTES

Valide Agent 365 en ambiente productivo controlado

Escenarios probados y evidencia para autorizar el uso de agentes con A365

Usted sabe qué capacidades de Agent 365 le interesan, pero aún no confirma cómo se comportan sus agentes de forma gobernada: hace falta validar escenarios predefinidos en un ambiente controlado.

Para ampliar su uso necesita evidencia confirmada del ciclo completo — descubrimiento, gobernanza, seguridad, identidad y protección de datos — con sus propios agentes y el proceso de gestión del cambio.

En el mercado, la magnitud de esa brecha ya se puede medir:

PUNTOS CIEGOS

82%

…hallaron agentes desconocidos en el último año

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

ACCESO EXTRA

53%

…tuvo agentes que excedieron los permisos previstos

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

VACÍO POL.

31%

…ya formalizaron una política de agentes

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

Valide funcionalidad y línea base de riesgo agéntico antes de escalar.

Esto entrega nuestra experiencia E-valuation: un conjunto predefinido de escenarios validados según sus propios requisitos.

E-valuation: valide Agent 365 antes de ampliar su uso

E-valuation valida Agent 365 en un ambiente productivo controlado mediante escenarios predefinidos, configurados y probados según sus requisitos. La actividad confirma la funcionalidad y establece una línea base para gestionar el riesgo agéntico antes de ampliar su uso.

La validación cubre el ciclo completo — descubrimiento, gobernanza, seguridad, identidad y protección de datos — y documenta hallazgos, ajustes y prioridades. Está dirigida a responsables de seguridad, TI y cargas de trabajo de Nivel 300 (TDM), en modalidad remota o híbrida.

- Alcance controlado para reducir la incertidumbre, anticipar impactos y validar el comportamiento antes de ampliar el uso.
- Criterio experto para definir configuración, controles de gobernanza y mejores prácticas según su contexto operativo.
- Escenarios predefinidos, ajustados a sus requisitos y validados con evidencia de funcionamiento y control.
- Resultados documentados, plan priorizado y presentación ejecutiva para definir condiciones de escalamiento.

SYNERGY ADVISORS

E-valuation

Agent 365 (A365) — Casos de uso de piloto productivo

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-valuation (piloto limitado: prueba / producción)

EXPERIENCIA BASE

Hasta **8** SESIONES — MÁX **4** SEMANAS

Experiencia Base

- ✓ Escenarios clave validados en 4 semanas como máximo
- ✓ Funcionalidad validada según sus requisitos
- ✓ Resultados de validación, plan y presentación ejecutiva

ALCANCE EXTENDIDO (PLUS)

Hasta **10** SESIONES — MÁX **5** SEMANAS

Alcance extendido (Plus)

- ✓ La misma validación, hasta 5 semanas
- ✓ Plan documentado de implementación y configuración en producción
- ✓ El plan se revisa con su equipo y Guía de operaciones

Alcance y entregables

Experiencia Base

EN ALCANCE

- ✓ Validación de escenarios predefinidos
- ✓ Hasta 8 sesiones en 4 semanas
- ✓ Funcionalidad validada según sus requisitos
- ✓ Revisión experta de configuración y gobernanza

FUERA DE ALCANCE

- ✕ Ambiente de laboratorio aislado
- ✕ Cambios adicionales en producción o en cargas no relacionadas
- ✕ Escenarios de desarrollo o integraciones a medida

ENTREGABLES

- ● Informe de validación
- ● Plan de implementación para producción
- ● Presentación ejecutiva

Alcance extendido (Plus)

EN ALCANCE

- ✓ Validación de escenarios predefinidos
- ✓ Hasta 10 sesiones en 5 semanas
- ✓ Plan de producción documentado, no aplicado
- ✓ Plan revisado con su equipo

FUERA DE ALCANCE

- ✕ Ambiente de laboratorio aislado
- ✕ Cambios aplicados en producción o en cargas no relacionadas
- ✕ Escenarios de desarrollo no listados

ENTREGABLES

- ● Informe de validación
- ● Plan de configuración para producción
- ● Guía general de operaciones

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-valuation

Dinámica de sesiones

01

Definir alcance

Usted acuerda el entorno, los objetivos y los criterios de éxito.

02

Validación en piloto limitado

Configura y valida escenarios predefinidos en laboratorio.

03

Revise control

Valida configuración y controles según prácticas recomendadas.

04

Pruebas de función

La funcionalidad y los escenarios se validan según sus requisitos.

05

Ordene impacto

Prioriza resultados por impacto y preparación para producción

06

Informe y cierre

Se presentan resultados de validación y el plan de producción.

Portafolio de experiencias: una ruta de gobernanza

ALINEAR, IDEAR

Crear alineación y acordar el modelo objetivo

E-nsights

E-nvision

PROBAR Y COMPROBAR

Demostrar y comprobar en un laboratorio dedicado

E-mmersion

E-xplorer

VALIDAR Y DECIDIR

Validar funcionalidad antes de producción

E-valuation

PILOTO — ESCALA

Pasar a producción y ampliar la gobernanza

E-Scuba

Decida el paso a producción con riesgo evaluado

Usted pasa a producción sabiendo exactamente cómo actúan sus agentes, dónde está el riesgo y qué necesita para gobernarlos a escala.

Menos incertidumbre y sorpresas; inversión enfocada donde más reduce el riesgo.

Demos juntos el siguiente paso.



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

Vea más... →