SYNERGY ADVISORS

E-nsights

GOBERNANZA DE AGENTES DE IA

Eventos y webinars dirigidos por expertos sobre gobernanza de agentes

La gobernanza no sigue el ritmo de los agentes

El interés por los agentes es real, pero no hay una visión consolidada de lo que son, nadie aprueba su acceso, y la adopción dentro de Microsoft 365 avanza más rápido que las decisiones de gobernanza que la respaldan.

Quienes deciden deben saber qué riesgos de agentes les aplican, qué impacto empresarial tienen y qué controles los mitigan, antes de que los agentes escalen en la organización.

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

PUNTOS CIEGOS

82%

...descubrieron agentes desconocidos en el último año

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

EXCESO DE ACCESO

53%

...han tenido agentes que exceden sus 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, hay que entender los riesgos.

Eso es lo que ofrecen nuestras experiencias E-nsights: sesiones dirigidas por expertos — webinar o evento — en formato empresarial o técnico.

Le presentamos Agent 365 E-nsights de Synergy Advisors

E-nsights es un conjunto de experiencias que Synergy Advisors ha creado para este momento: sesiones dirigidas por expertos sobre las mejores prácticas para la mitigación de riesgos, gobernanza y gestión de los agentes, con el contenido adaptado a su madurez y prioridades de antemano.

Existe para que comprenda los riesgos, su impacto empresarial y los controles que los mitigan, y decida con claridad antes de su adopción. Impartido como webinar o presencial para ejecutivos de Nivel 200 (BDM) y equipos técnicos de Nivel 300 (TDM); la siguiente página detalla cómo se desarrollan las sesiones.

- Descubrimiento de agentes, gobernanza, seguridad y cumplimiento, cubierto de principio a fin.
- Los controles que mitigan los riesgos de agente más comunes, guiados por un experto.
- Hasta 3 casos de uso comunes de agentes revisados, y dónde fallan en la práctica.
- Demos en vivo sobre escenarios de agentes preconfigurados, más integración con otras tecnologías.

Agent 365 (A365) – Escenarios 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 de E-nsights (Eventos y Webinars)

SESIÓN EJECUTIVA (BDM)

Hasta **2h** POR SESIÓN

Hasta **3** CASOS DE USO

Sesión Ejecutiva (BDM)

- ✓ Mejores prácticas expertas para la mitigación de riesgos, gobernanza y gestión de agentes
- ✓ Visión clara de los riesgos, controles y casos de uso más comunes de los agentes
- ✓ Impacto empresarial planteado antes de comprometerse con la adopción o implementación

SESIÓN TÉCNICA (TDM)

Hasta **3h** POR SESIÓN

Hasta **3** CASOS DE USO

Sesión Técnica (TDM)

- ✓ Recorrido experto por los controles que mitigan los principales riesgos de agentes
- ✓ Hasta 3 casos de uso comunes, con demos en vivo de gobernanza
- ✓ Punto de partida definido antes de la adopción o implementación

Alcance y entregables

Sesión Ejecutiva (BDM)

EN ALCANCE

- ✓ 1 sesión de hasta 2 horas, formato empresarial
- ✓ Webinar o presencial, con un experto en gobernanza
- ✓ Contenido adaptado a su madurez y prioridades
- ✓ Participantes ilimitados por webinar; aforo del recinto si es presencial

FUERA DE ALCANCE

- × Sesiones adicionales o talleres de seguimiento
- × Cambios o configuración en cualquier entorno
- × Laboratorios, inmersiones profundas o evaluaciones
- × Desarrollo personalizado o integraciones

ENTREGABLES

- ● Presentación con conceptos clave y visuales
- ● Grabación completa, en menos de 1 semana

Sesión Técnica (TDM)

EN ALCANCE

- ✓ 1 sesión de hasta 3 horas, formato técnico
- ✓ Hasta 3 casos de uso comunes revisados, y dónde fallan
- ✓ Demos en vivo sobre escenarios preconfigurados e integraciones
- ✓ Contenido adaptado a su madurez y prioridades

FUERA DE ALCANCE

- × Sesiones adicionales o talleres de seguimiento
- × Cambios o configuración en cualquier entorno
- × Laboratorios, inmersiones profundas o evaluaciones
- × Desarrollo personalizado o integraciones

ENTREGABLES

- ● Presentación con conceptos clave y visuales
- ● Grabación completa, en menos de 1 semana

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-nsights

Cómo se desarrollan las sesiones

01

Público y objetivos

Público objetivo y objetivos empresariales confirmados antes de la sesión.

02

Contenido a medida

Materiales adaptados a su madurez y prioridades.

03

Sesión de casos de uso

Capacidades, beneficios y escenarios de alto impacto cubiertos, hasta 3 casos de uso.

04

Demo en vivo

Demos sobre escenarios preconfigurados, más integración con otras tecnologías.

05

Debate abierto

Preguntas, respuestas y futuras áreas de exploración.

06

Traspaso

Presentación y grabación de la sesión entregadas a sus equipos.

Un portafolio de experiencias, un único recorrido de gobernanza

ALINEAR & DISEÑAR

Cree alineación y acuerde el modelo objetivo

E-nsights

E-nvision

EXPERIMENTAR & DEMOSTRAR

Muestre que funciona y pruébelo en un laboratorio dedicado

E-mmersion

E-xplorer

VALIDAR & DECIDIR

Valide la funcionalidad antes de producción

E-valuation

PILOTAR & ESCALAR

Pase a producción y escale la gobernanza

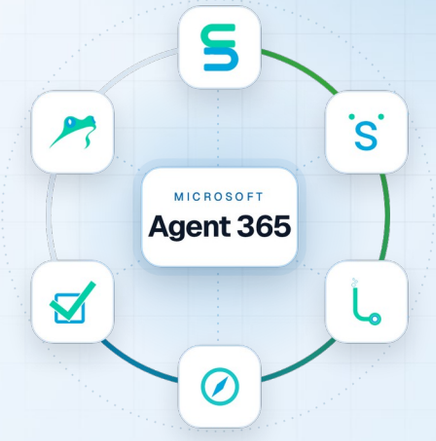
E-Scuba

Decida con evidencia, no con suposiciones

Sale sabiendo qué riesgos de agente le afectan, quién debe gobernarlos y el impacto empresarial de cada uno.

La cuestión ya no es si el riesgo es real, sino qué control viene primero.

Demos el siguiente paso juntos.



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

Más información →