BeyondTrust

Más Allá del Perímetro Humano

Dominando la explosión de identidades no humanas y agentes de IA

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

La Anatomía de Una Identidad no Humana

Un Ecosistema Diverso

Incluye **Cuentas de Servicio** (aplicaciones heredadas), **claves API** (integraciones en la nube), **secretos** (canalizaciones de DevOps) y **tokens** OAuth.

La nueva función: Agentes de IA

Agentes autónomos que no solo siguen un guion, sino que toman decisiones y ejecutan flujos de trabajo de varios pasos en tus aplicaciones SaaS.

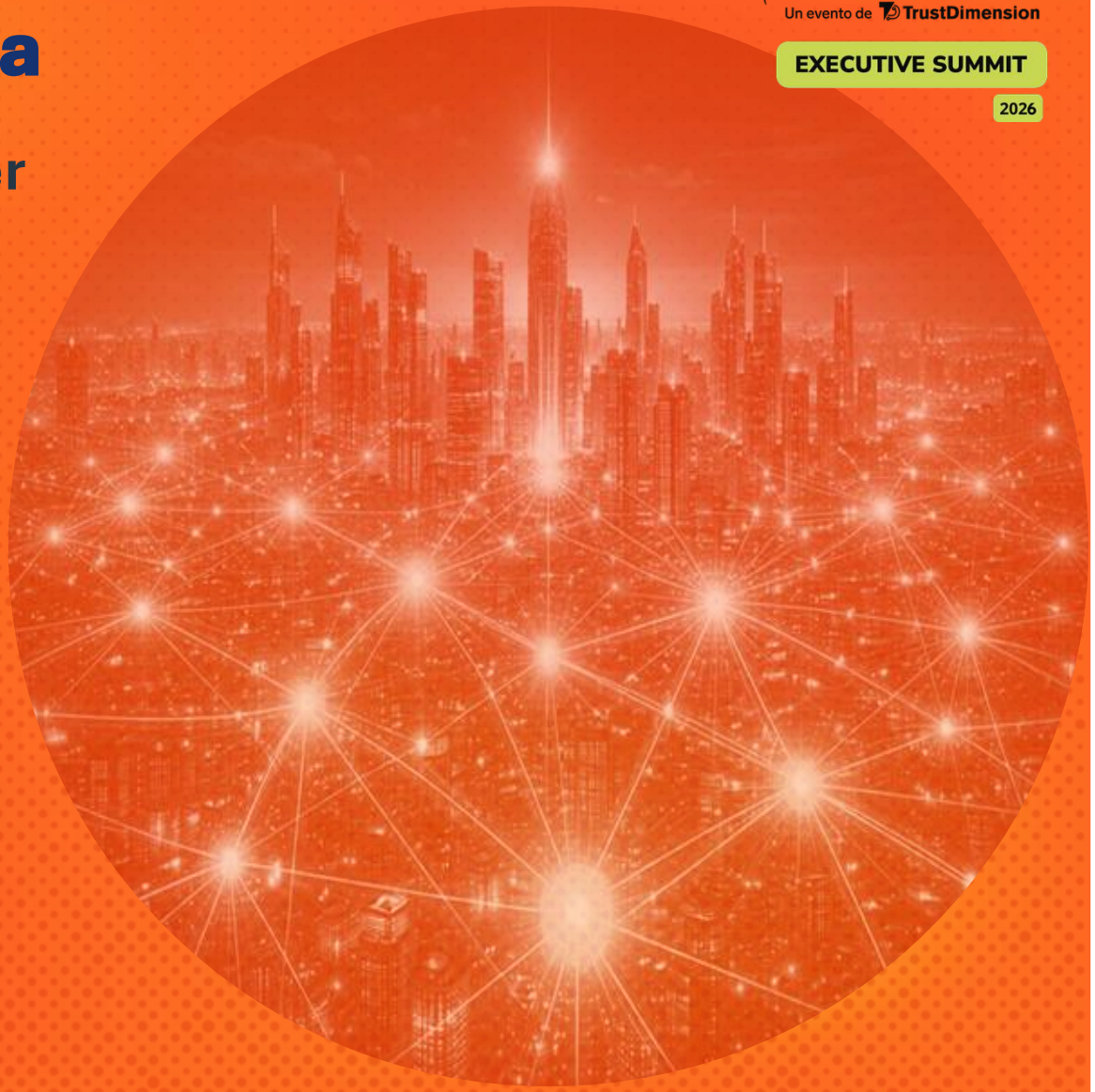
La Brecha de Seguridad

A diferencia de los humanos, los NHIs no tienen datos biométricos, no utilizan autenticación multifactor y nunca duermen, lo que los convierte en el objetivo más fácil para los atacantes modernos.

La realidad 100:1

Su Nueva Población Mayoritaria

- El cambio de un **perímetro centrado en el ser humano** a una superficie de ataque **centrada en la máquina** carece de herramientas integrales de seguridad de identidades.
- El acceso y el almacenamiento tradicionales de PAM siguen siendo necesarios, pero ya no son suficientes para **cargas de trabajo efímeras**.
- Las NHIs paralelas a menudo se crean fuera de la **supervisión de TI y la gestión de accesos**.



inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

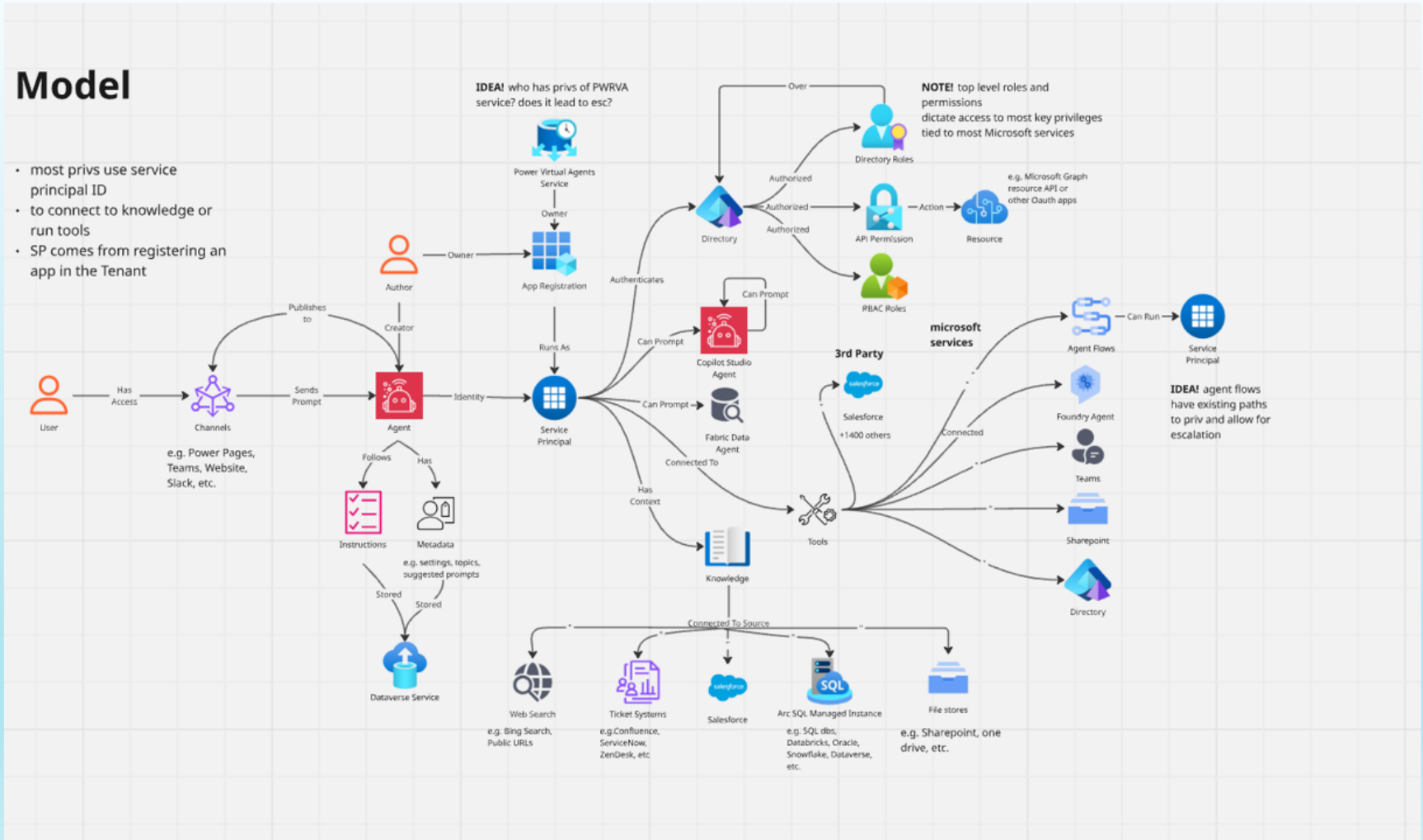
Agentes de IA

El Auge del Empleado Autónomo

- Agentes de IA: Sistemas autónomos (p. ej., CoPilot, Salesforce Agentforce) que actúan en su nombre.
- Nuevos riesgos como la inyección de mensajes pueden provocar una escalada de privilegios no autorizada.
- Estos agentes suelen eludir la autenticación multifactor estándar y los controles de seguridad tradicionales.

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Alcance de los Agentes de IA



Secretos

Las Identidades “Fantasma" Que Acechan Su Código

- La crisis de la **proliferación de secretos**: miles de credenciales ocultas en GitHub, Jira y Slack.
- **Los secretos estáticos** son el principal objetivo de los atacantes que buscan moverse lateralmente.
- La transición de la **gestión de secretos** a la gobernanza de secretos.

Secretos

Las claves API, los tokens OAuth y las claves SSH son las "contraseñas" del mundo no humano, pero a menudo están codificadas de forma fija y se olvidan.

¿Por qué se Está Rompiendo la Seguridad de las Identidades?

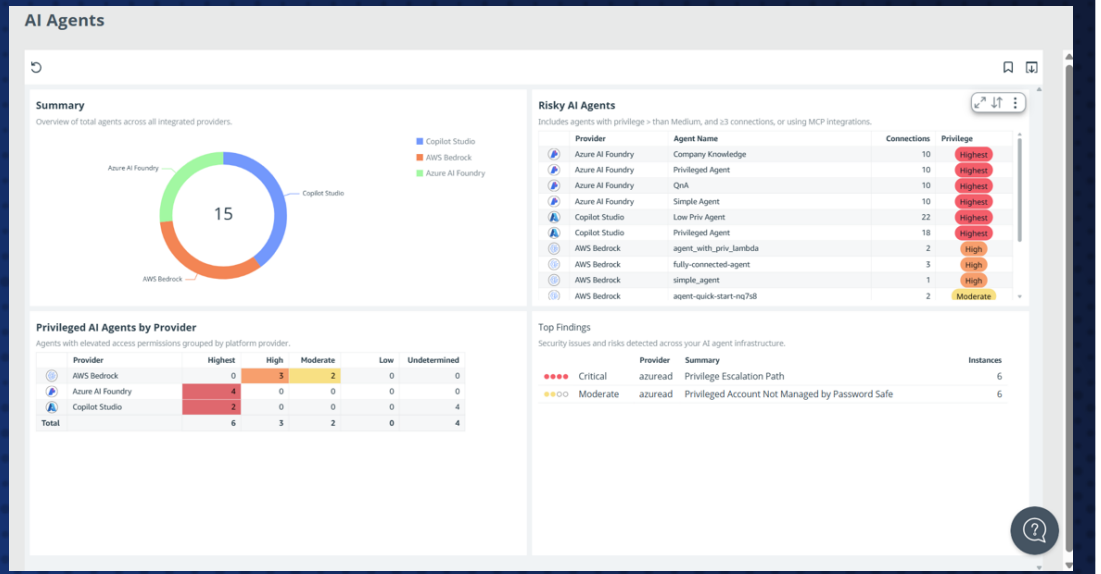
inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

- Los atacantes piensan en **vistas gráficas y conectadas**.
- Los defensores piensan en **listas ordenadas**, **pero incompletas**.
- **Las herramientas fragmentadas** no pueden crear el contexto necesario para defenderse.


Ambientes
On-Prem
Nube híbrida
Nube y SaaS
Kubernetes
La mayoría de las filtraciones comienzan con una vulneración de las identidades.
Identidades
Humano
Carga de trabajo
Máquina
Agente
(NHI)
Activos
Servidores
Contenedores
Sin servidor
Dispositivos
ICS/OT

La Brecha de Visibilidad
Por qué el PAM Tradicional no Puede ver el Recorrido Completo

- **Silos de identidad**: las brechas entre dominios generan riesgos de seguridad.
- El peligro de los **privilegios indirectos**: las cuentas NHI de bajo nivel pueden conducir a accesos de administrador global.
- El **descubrimiento** debe ser continuo, no un escaneo trimestral.



El sistema PAM tradicional asegura la "puerta de entrada" pero pasa por alto los canales laterales ocultos.

Identidades No Humanas

Elevando el Nivel de Preparación Para las Auditorías

- El **gran volumen de identidades** hace que la preparación de auditorías sea más laboriosa y difícil.
- La mayoría de las herramientas de seguridad no parten de una **mentalidad orientada al cumplimiento normativo** ni ofrecen visibilidad en este sentido.
- Los auditores estarán **bajo presión** para establecer una base de referencia para el cumplimiento de las identidades no humana.

Unresolved Findings by MITRE ATT&CK® Mappings & Severity (Last 30 Days)

MITRE Tactic	MITRE Technique	Critical	High	Moderate	Low
Privilege Escalation	Account Manipulation	11	0	0	0
Credential Access	Credentials from Password Stores	0	0	4	0
Execution	Exploitation for Client Execution	0	0	7	0
Credential Access	Steal or Forge Kerberos Tickets	0	0	44	0
Credential Access	Unsecured Credentials	0	137	0	0
Initial Access	Valid Accounts	0	12	41	31
Privilege Escalation	Valid Accounts	0	0	10	0

La Solución BeyondTrust

Identity Security Insights

Un evento de TrustDimension

EXECUTIVE SUMMIT 2026

- **Visibilidad centralizada** en todos los proveedores de identidad (Okta, Entra ID) y en la nube (AWS, Azure, GCP).
- **Detección en tiempo real** de amenazas y configuraciones incorrectas basadas en las identidades.
- **Recomendaciones prácticas,** desde la identificación del riesgo hasta su priorización para la mitigación del mismo.

Transición de la gestión reactiva de identidades a una gestión proactiva basada en IA a través de la plataforma Pathfinder para una mayor higiene de identidades y un mejor cumplimiento normativo.

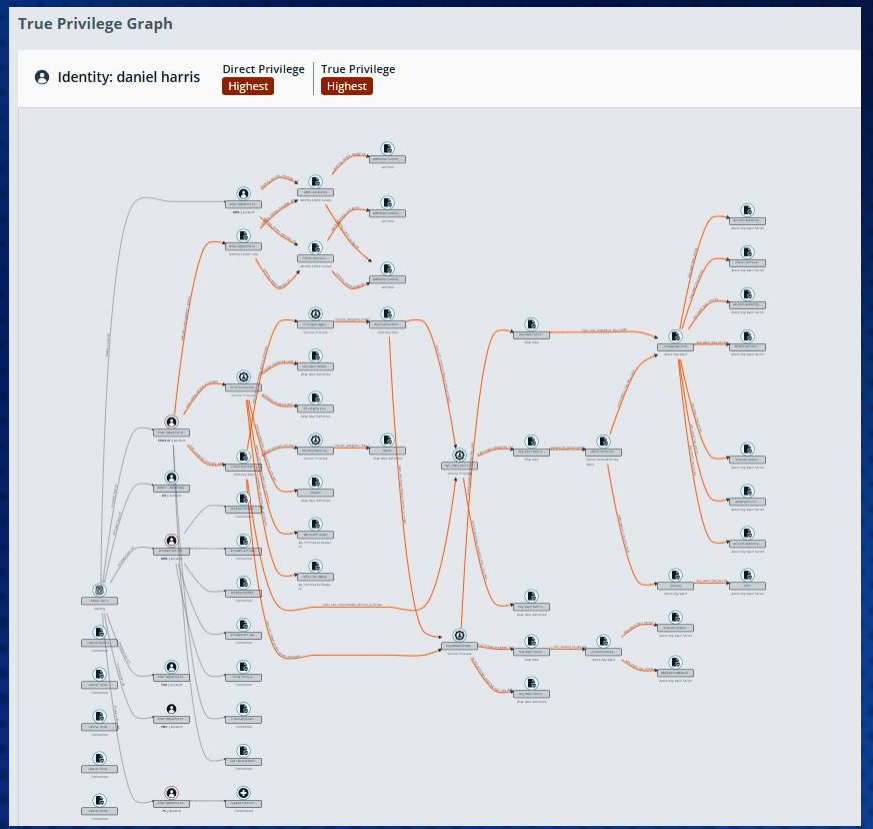
Seguridad de Identidades con Agentes de IA

1. **Inteligencia de agentes**: ¿Cuántos agentes existen y dónde?
2. **Acceso de los agentes:** ¿Qué datos pueden acceder los agentes?
3. **Footprint de los Agentes:** Qué agentes pueden iniciar
4. **Seguridad de los Agentes:** Riesgo, gravedad y recomendaciones
5. **Gráfico de Seguridad de los Agentes:** Rutas de privilegios y riesgos de escalada

El Gráfico True Privilege™

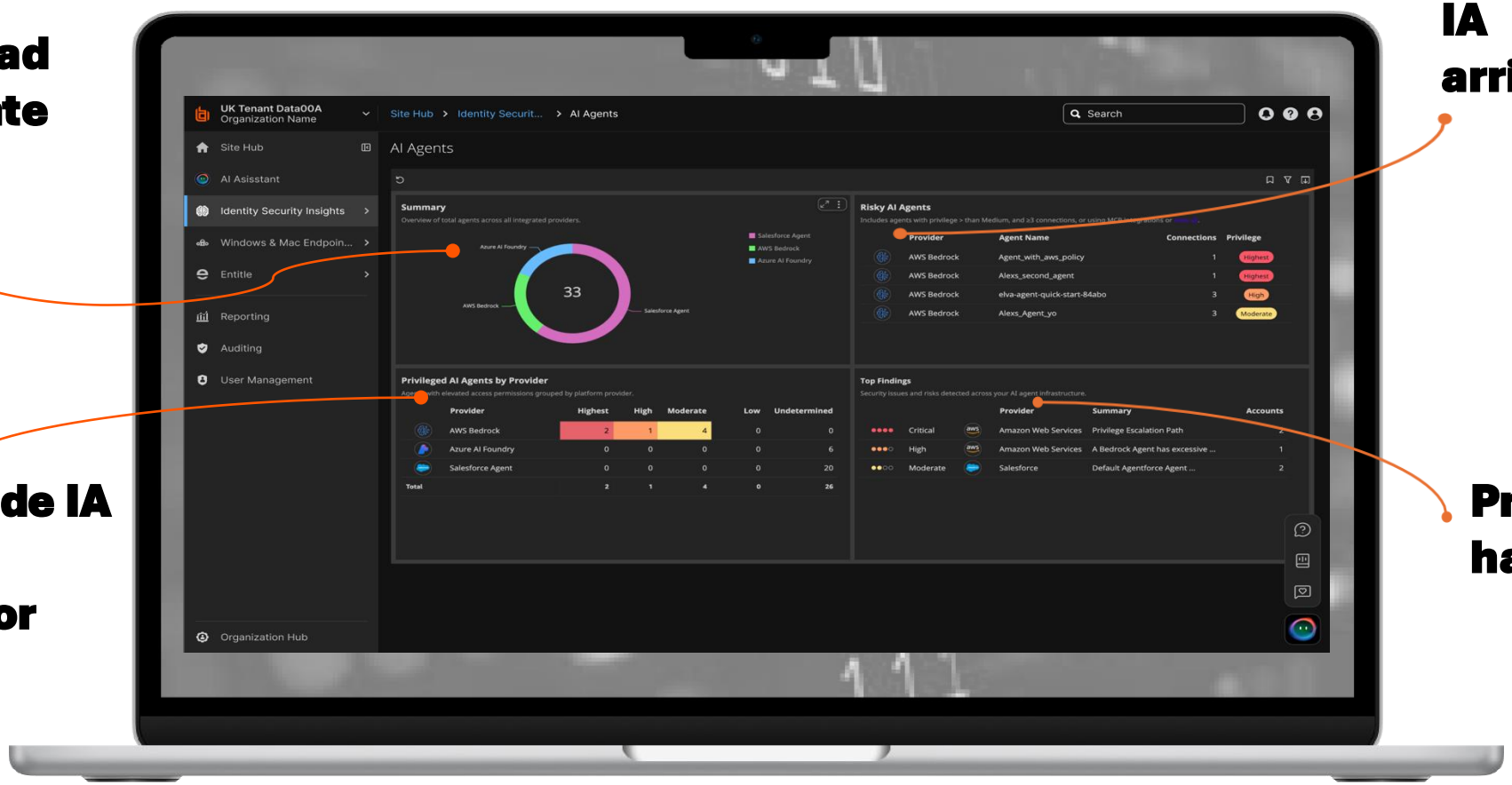
Para proteger lo que no puedes ver, necesitas un mapa visual de todas las posibles rutas de escalada a través de tus identidades.

- Visualizando las complejas interconexiones entre humanos, máquinas e IA
- Descubriendo las "vías ocultas hacia el privilegio" que conectan los sistemas locales con la nube
- Contextualizando el riesgo: Saber no solo quién tiene acceso, sino también qué pueden hacer realmente.



Visibilidad del Agente de IA

Agentes de IA por proveedor



Agentes de IA arriesgados

Principales hallazgos

INSIGHTS

Insights Cuenta con Telemetría de IA Completa

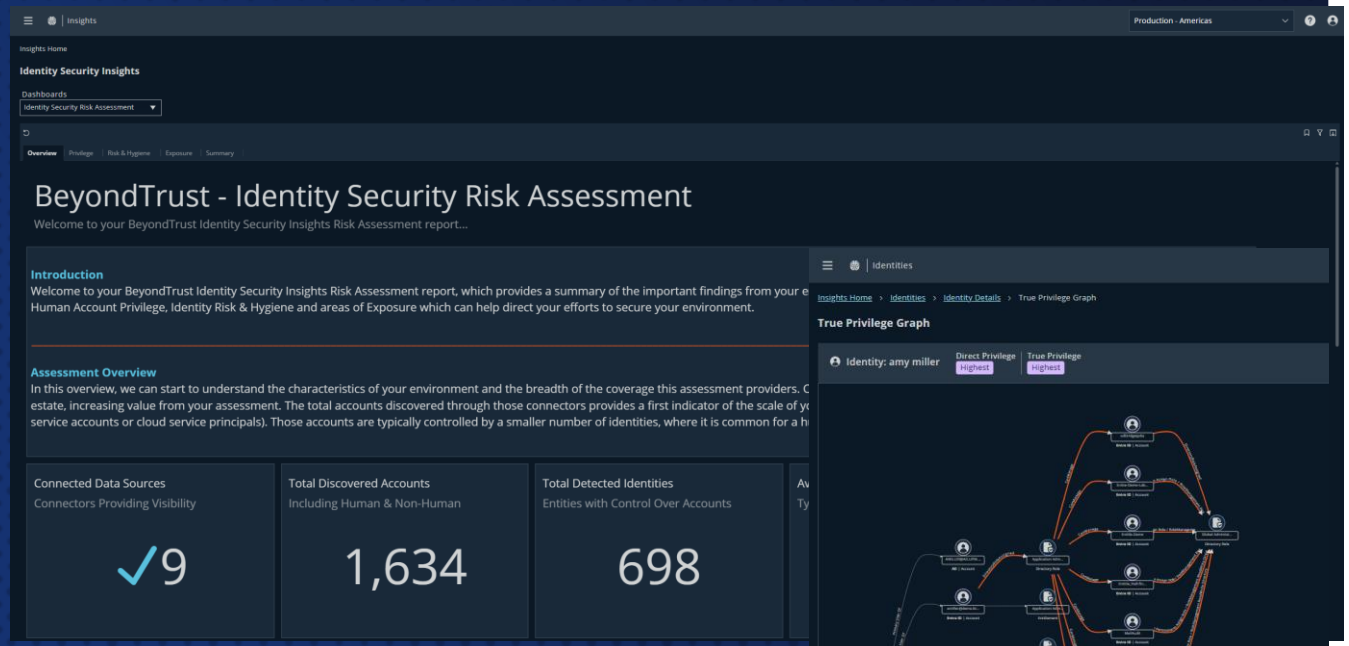
Los 10 Principales Proveedores de IA Corporativa

Ranking	Plataforma/Servicio de IA	Proveedor	Connector
1	Copilot (incl. Copilot Studio)	Microsoft	✅
2	ChatGPT Enterprise	OpenAI	✅
3	OpenAI Admin	OpenAI	✅
4	Bedrock	AWS	✅
5	Vertex AI	Google	✅
6	Gemini	Google	SOON
7	Agentforce / Einstein	Salesforce	✅
8	ServiceNow AI	ServiceNow	✅
9	Claude	Anthropic	SOON
10	Databricks AI / Mosaic / Agents	Databricks	✅

Identity Security Risk Assessment

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

- **Evaluación de riesgos** complementaria y sin compromiso.
- **Configuración sencilla** mediante conectores de solo lectura en menos de una hora.
- En 24 horas, el panel de control revela identidades, privilegios y rutas críticas.
- Identifique cuentas de administrador en la sombra con altos privilegios reales: las vulnerabilidades que de otro modo pasarían desapercibidas.
- Reciba recomendaciones para mejorar la seguridad de su identidad y el cumplimiento normativo.



inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Tu peor día siempre puede empeorar.

Los atacantes **tendrán** las credenciales.

Lo que suceda después **es controlable**.

Gracias

Carlos Ochoa
Territory Manager
+ 52 55 5457 5142
cochoa@beyondtrust.com

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

beyondtrust.com

Erick Robles
Solutions Engineer, LATAM
+ 52 55 4043 0553
erobles@beyondtrust.com