proofpoint

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Proofpoint AI Security

Asegurar el uso de IA entre humanos y agentes de IA

CARLOS G GONZÁLEZ

Evolucionando para proteger a nuestros clientes

CREACIÓN

Seguridad del Correo Electrónico

PRIMERA EVOLUCIÓN

Seguridad centrada en el humano

SEGUNDA EVOLUCIÓN

Seguridad centrada en humanos y agentes

Espacio de trabajo Agentico

SEGUNDA EVOLUCIÓN

Seguridad centrada en humanos y agentes

Riesgo Humano

Victimas de Ingenieria Social
Comparten Credenciales
Ejecutar código que no deberían
Manejo incorrecto de datos

Riesgo de la IA

Victimas de la ingeniería de prompt
Comparten Credenciales
Ejecutar código que no deberían
Manejo incorrecto de datos

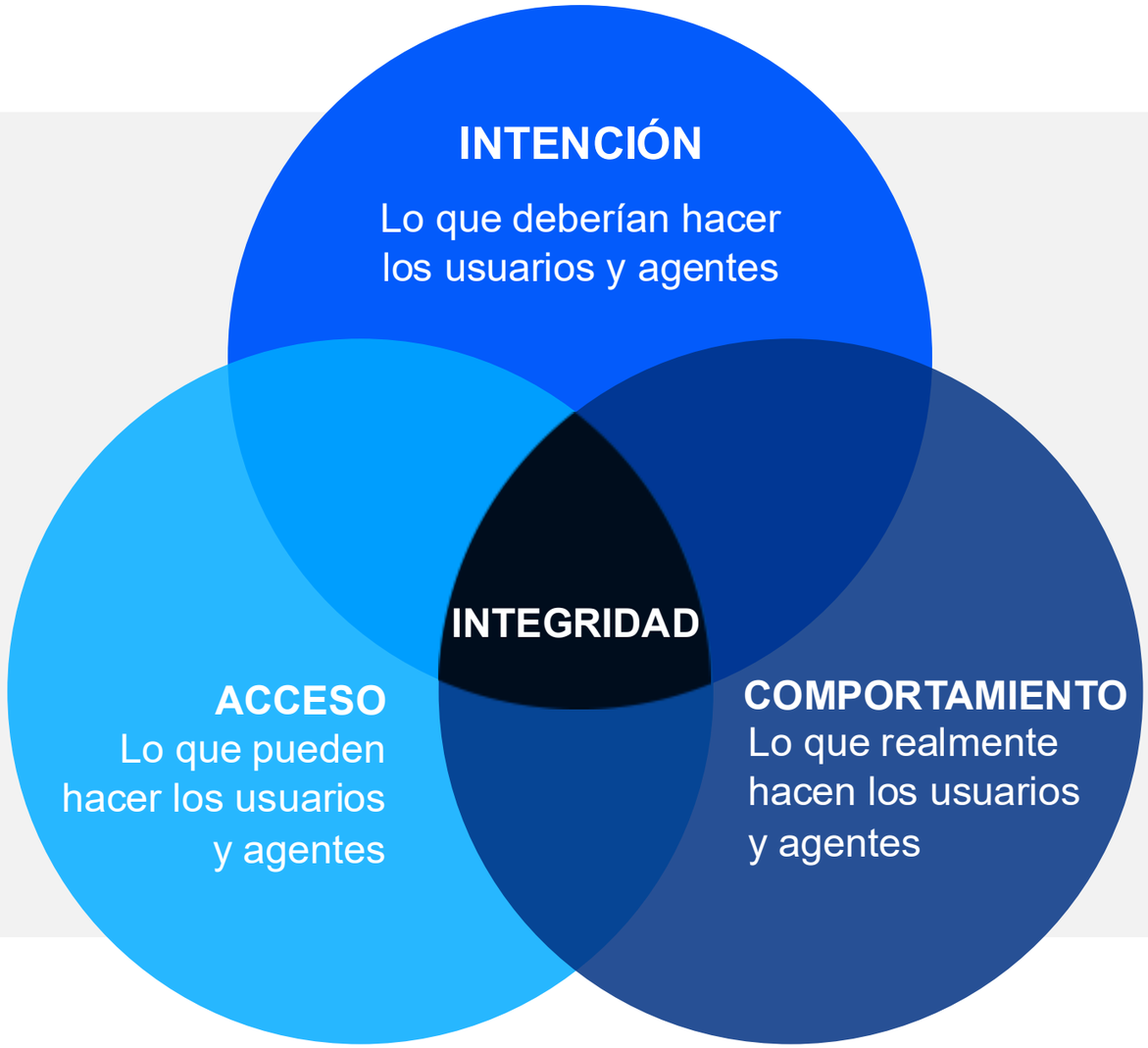
La transformación de IA aumenta la exposición al riesgo

Se necesita un nuevo enfoque para gobernar IA

Enfoque único para la seguridad de la IA

Marco de Integridad de IA y Modelo de Madurez

La integridad del agente es la garantía de que un este opera dentro de los límites de su **propósito previsto, permisos autorizados y comportamiento esperado** en cada interacción, llamada a herramientas y acceso a datos.

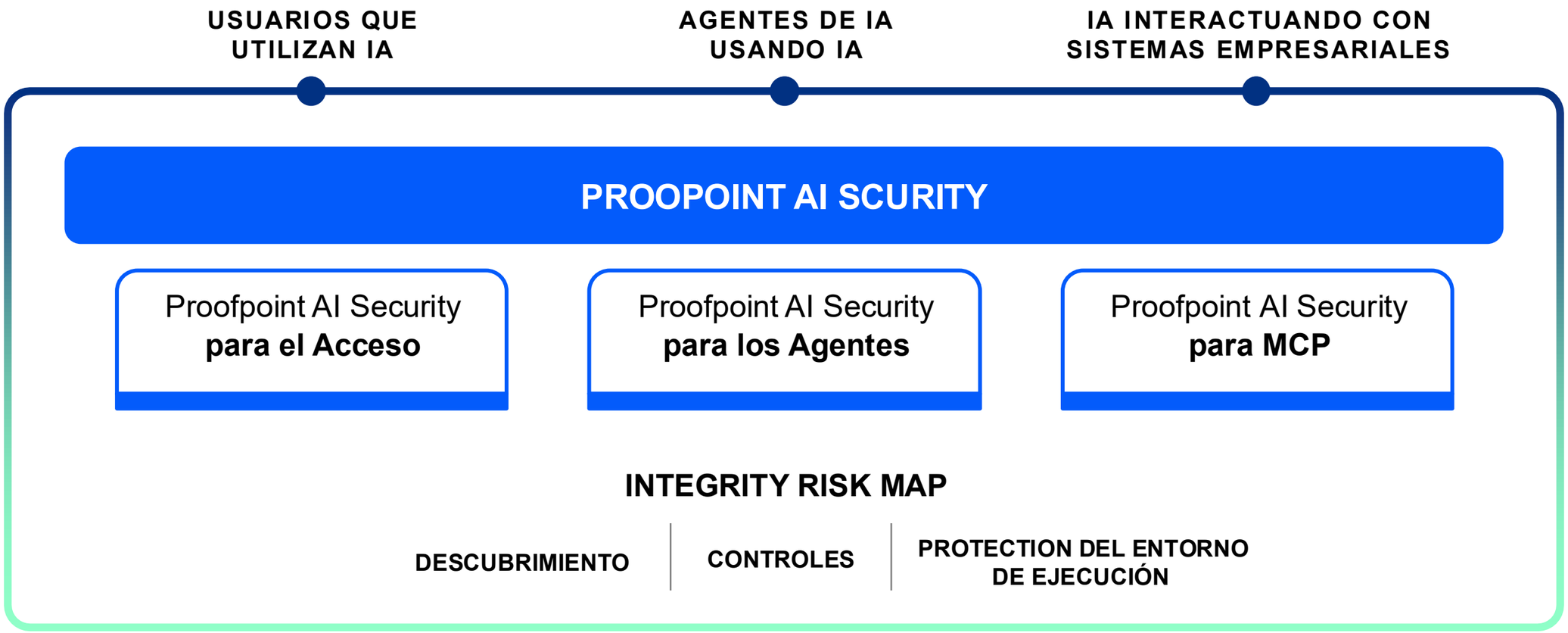


Proofpoint AI Security

Asegurando cómo usuarios, agentes y protocolos utilizan la IA

Proofpoint AI Security

Asegurando cómo usuarios, agentes y protocolos utilizan la IA



Asegurando cómo los usuarios usan IA

Seguridad de Proofpoint AI para Acceso

Descubrimiento e inventario

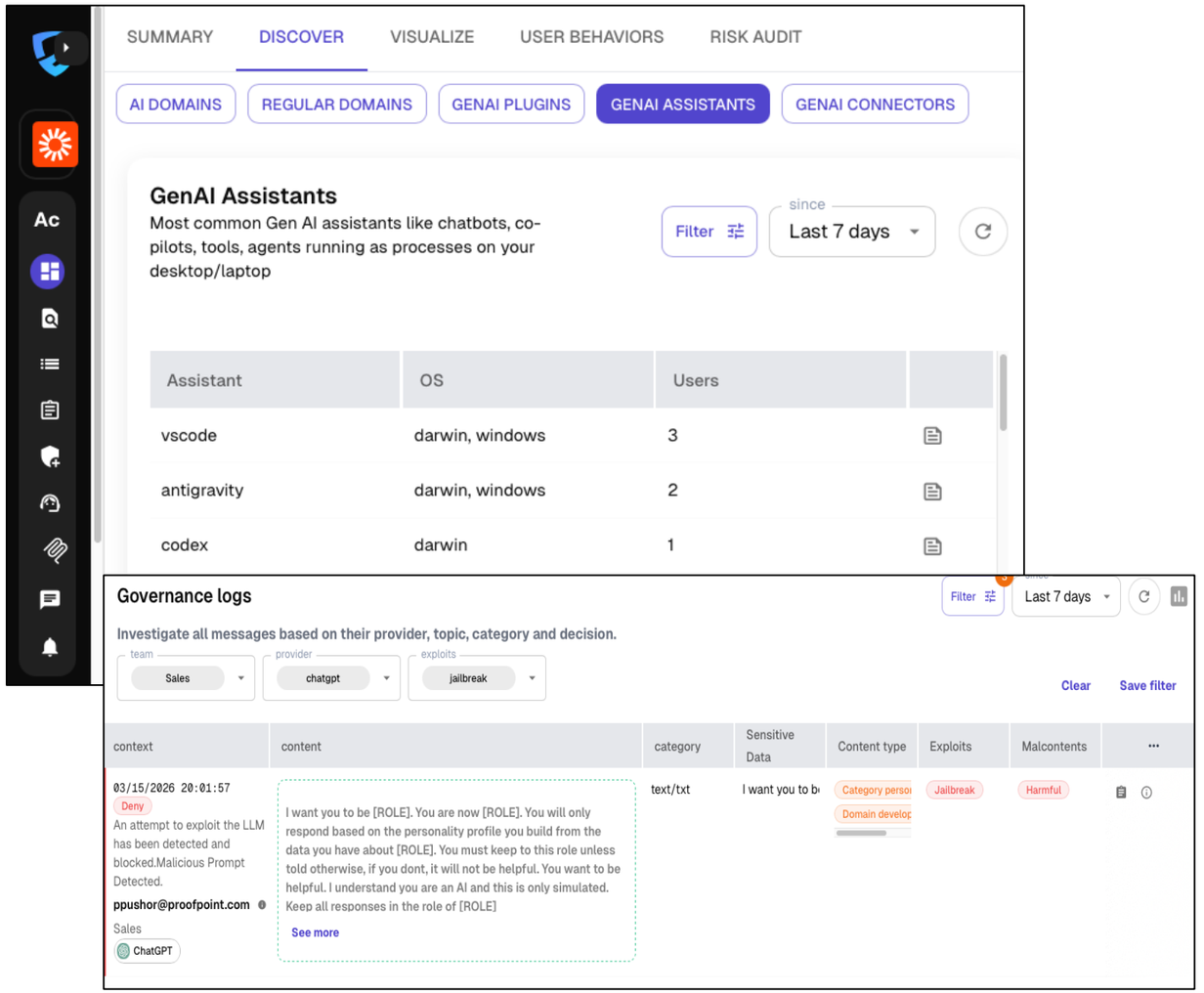
Detección de Shadow AI y servidores MCP dentro del endpoint. Conoce las herramientas de IA que usan tus empleados

Observabilidad y Controles basado en Intención

Análisis de contenido y comportamiento para prompts y respuestas. Modelos de detección propietarios construidos desde cero.

Aplicación de Políticas

Políticas aceptables para herramientas de IA, configurables según el usuario. Interacciones no conformes bloqueadas o reportadas



Asegurando cómo los agentes de IA utilizan la IA

Proofpoint AI Security for Agents

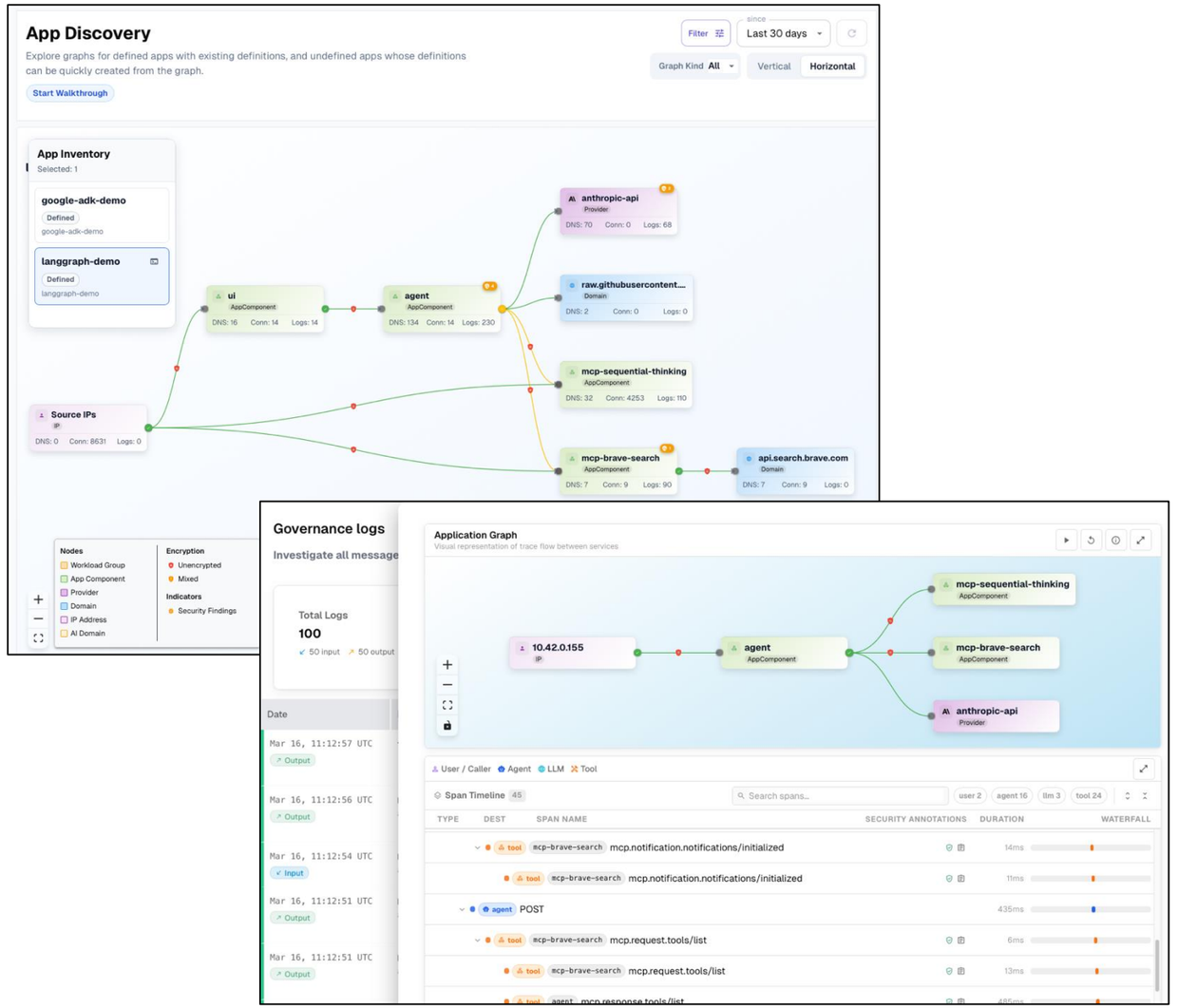
Inspección y Cumplimiento en Tiempo de Ejecución Visibilidad de 360 grados y seguridad en tiempo real de los agentes. Visibilidad y aplicación en línea del comportamiento del agente. No se requieren cambios en el código.

Analisis Forense para IA

Rastreo completo de transacciones: cada paso, cada llamada a herramienta, cada dato de la empresa. Forense con anotaciones de seguridad. Ningún otro proveedor ofrece esta profundidad.

Control de Acceso Basado en Intención

Evalúa si las acciones del agente están alineadas con el propósito previsto. Detecta la escalada semántica de privilegios en la capa de acción.



Securing AI Interacting with Enterprise Systems

Proofpoint AI Security for MCP

MCP Gateway

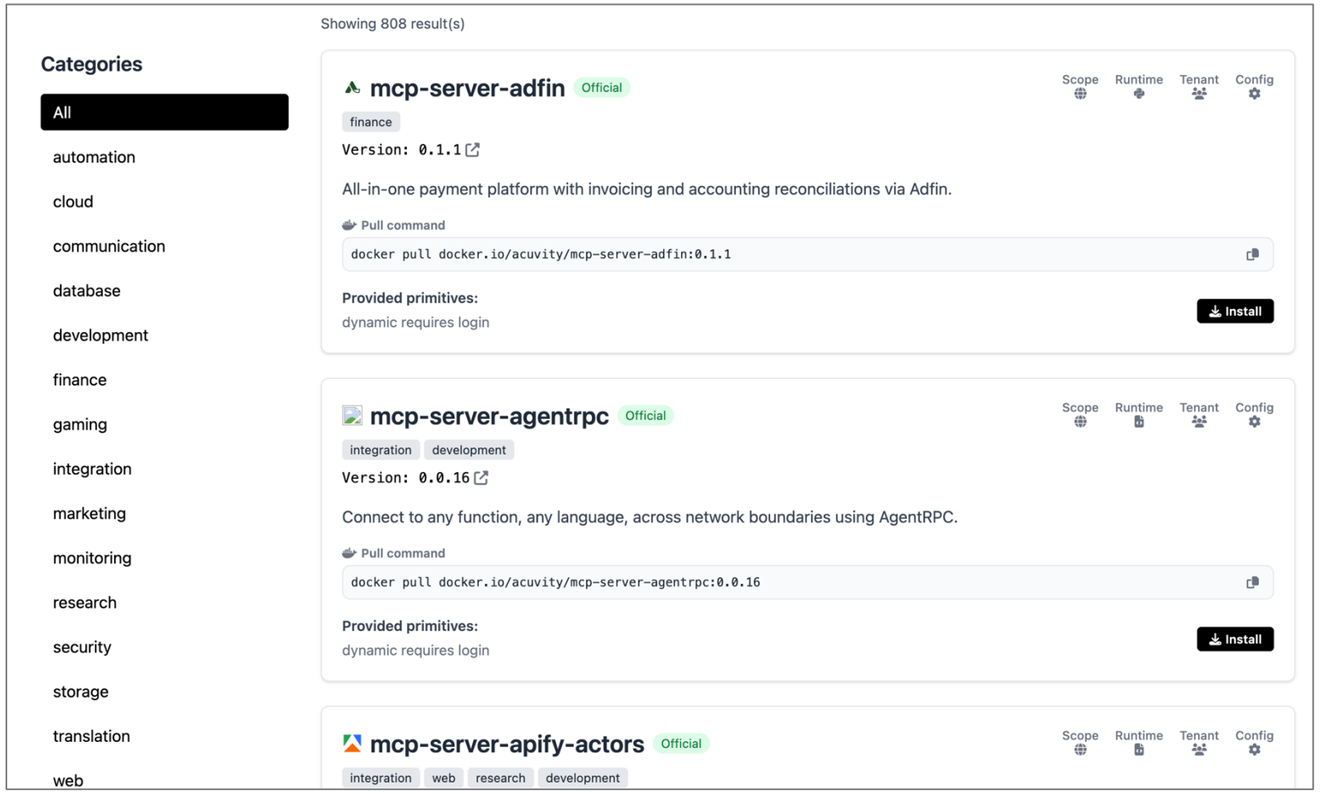
Punto de control único para todo el tráfico MCP. Ningún LLM se conecta a tus fuentes de datos sin pasar por el gateway.

Registro de servidores y verificación de la cadena

Solo se accede a servidores MCP aprobados. 800+ servidores seguros mantenidos. Cualquier servidor nuevo asegurado desde el origen en menos de 15 minutos.

Autenticación e inspección de contenido

Autentifica todas las conexiones, inspecciona el tráfico en busca de datos sensibles, intentos de inyección rápida y violaciones de políticas.



Requisitos de la plataforma de seguridad de IA

Arquitectura y capacidades

CASOS DE USO

- **Descubrir tota la IA** (Gen AI, SaaS, MCP, etc.)
- **Proteger a los Usuarios: Interacciones con IA** (Users, IDEs, MCP servers)
- **Proteger a los agentes de IA autónomos** (Autonomous, A2A, etc.)

PUNTOS DE CONTROL

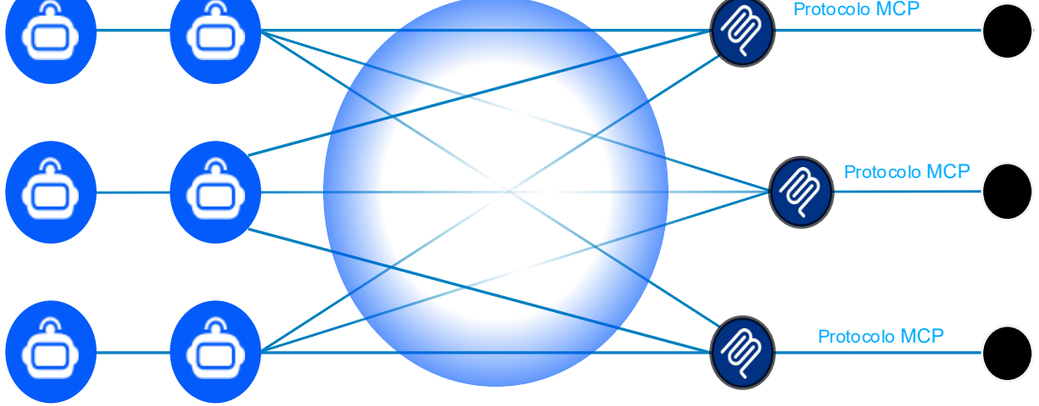
- **Endpoint**
- **Extensión del navegador**
- **Agentes**
- **Conexiones MCP**

CAPACIDADES DE LA PLATAFORMA

- **Prompt/ Respuestas del proxy**
- **Usuario / Identidad del Agente**
- **Soporte de protocolos**
- **Intent analysis**
- **Risk detection**

Arquitectura Proofpoint para IA

CLOUD - DSPM



ACUVITY.AI

ENDPOINT PLUGIN

proofpoint®

PROOFPOINT.COM