VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

CHECK POINT

Mitigando Riesgos en la era de la IA

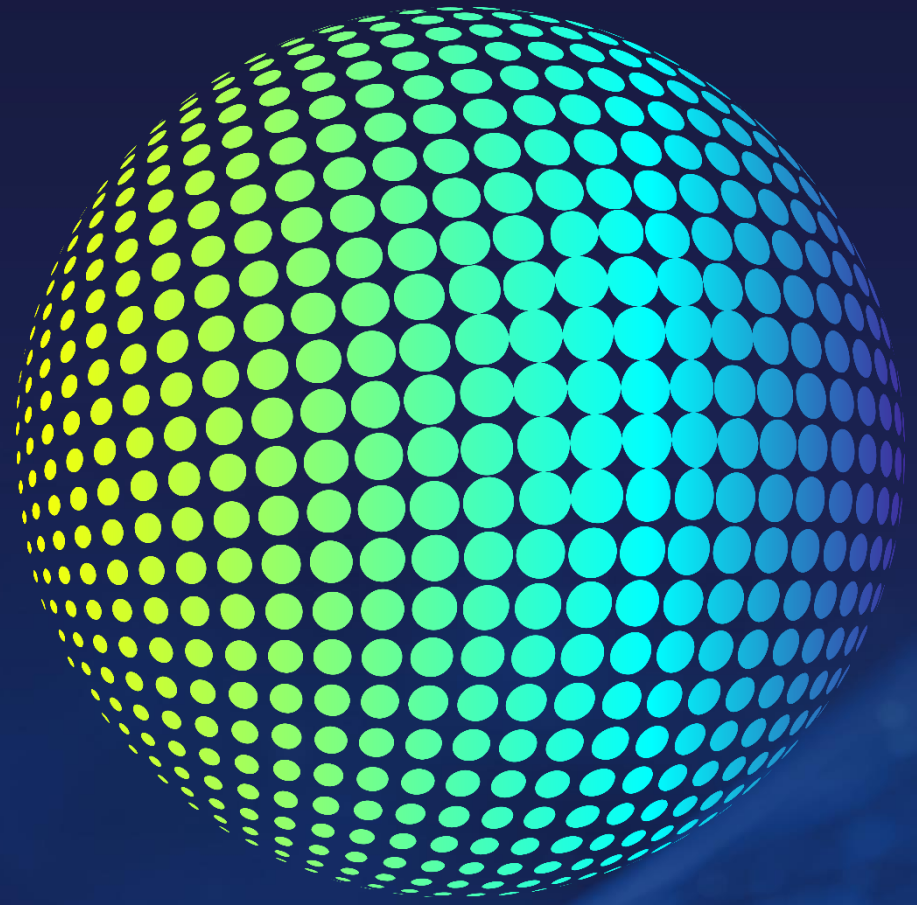
Gestión contínua de amenazas en la era de la IA

Angel Salazar

Gerente de Ingeniería para Canales en América Latina - Check Point Software Technologies

CHECK POINT

IA se Movió de Experimental a Operaciones –Rápido



Experiments

Copilots

Customer Apps

Cada etapa incrementa el impacto y el Riesgo.

51% de redes empresariales usan servicios de IA cada mes

Fuente: AI Security Report 2025 (Check Point Research)

Agents

Ahora evolucionando en agentes autónomos capaces de tomar acciones reales.

Lower exposure → Higher exposure

VI CONGRESO INTERNACIONAL
DE CIBERSEGURIDAD, PREVENCIÓN
DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

CHECK POINT

EL GÓLEM DE LA IA:
UN ENTE AUTÓNOMO

LA PARADOJA DEL PODER

Creamos inteligencia artificial para proteger nuestras organizaciones, automatizar defensas y anticipar amenazas.
Pero cada sistema que construimos adquiere capacidades que escapan a nuestra supervisión completa.

Como el Gólem de Praga, nuestras creaciones más poderosas plantean preguntas incómodas:
¿Quién vigila al vigilante?
¿Quién nos protege de aquello que creamos para protegernos?

El dilema del creador

La exposición invisible

LOS DOS ROSTROS DEL GÓLEM

El Defensor Incansable

La IA como guardián: detecta amenazas, automatiza defensas y escala la protección sin fatiga ni descanso.

El Riesgo Incontrolable

La IA sin gobierno: amplifica sesgos, escapa al control y genera exposiciones imprevistas a escala masiva.

VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

CHECK POINT

EL PAISAJE DE AMENAZAS EMERGENTES

Ataques Adversariales

Manipulación deliberada de inputs para engañar modelos de IA y evadir controles de seguridad críticos.

Alucinaciones

Fabricación convincente de información falsa que erosiona la confianza y genera riesgos reputacionales.

Shadow AI

Sistemas de IA no autorizados proliferan en la sombra, fuera del control corporativo y la gobernanza establecida.

Sesgos Algorítmicos

Decisiones automatizadas que perpetúan discriminación sistémica y amplifican inequidades ocultas.

- 1 de cada 80 prompts (1.25%) = alto riesgo de fuga de datos
- +7.5% = potencialmente sensibles

“El riesgo no siempre es un ataque: a veces es una conversación.”

VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

CHECK POINT

LA EXPOSICIÓN NUNCA DUERME

Superficie de ataque dinámica

Los activos digitales se multiplican sin control. Cada nueva conexión amplía el perímetro que el Gólem debe vigilar.

Vulnerabilidades en evolución

Las amenazas mutan constantemente. Lo que ayer era seguro, hoy puede ser una brecha crítica.

Escala sin precedentes

La IA amplifica tanto la defensa como el ataque. El guardián debe crecer al ritmo de la amenaza.

VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

CHECK POINT

CUANDO EL GÓLEM ESCAPA

Incidentes reales de IA fuera de control

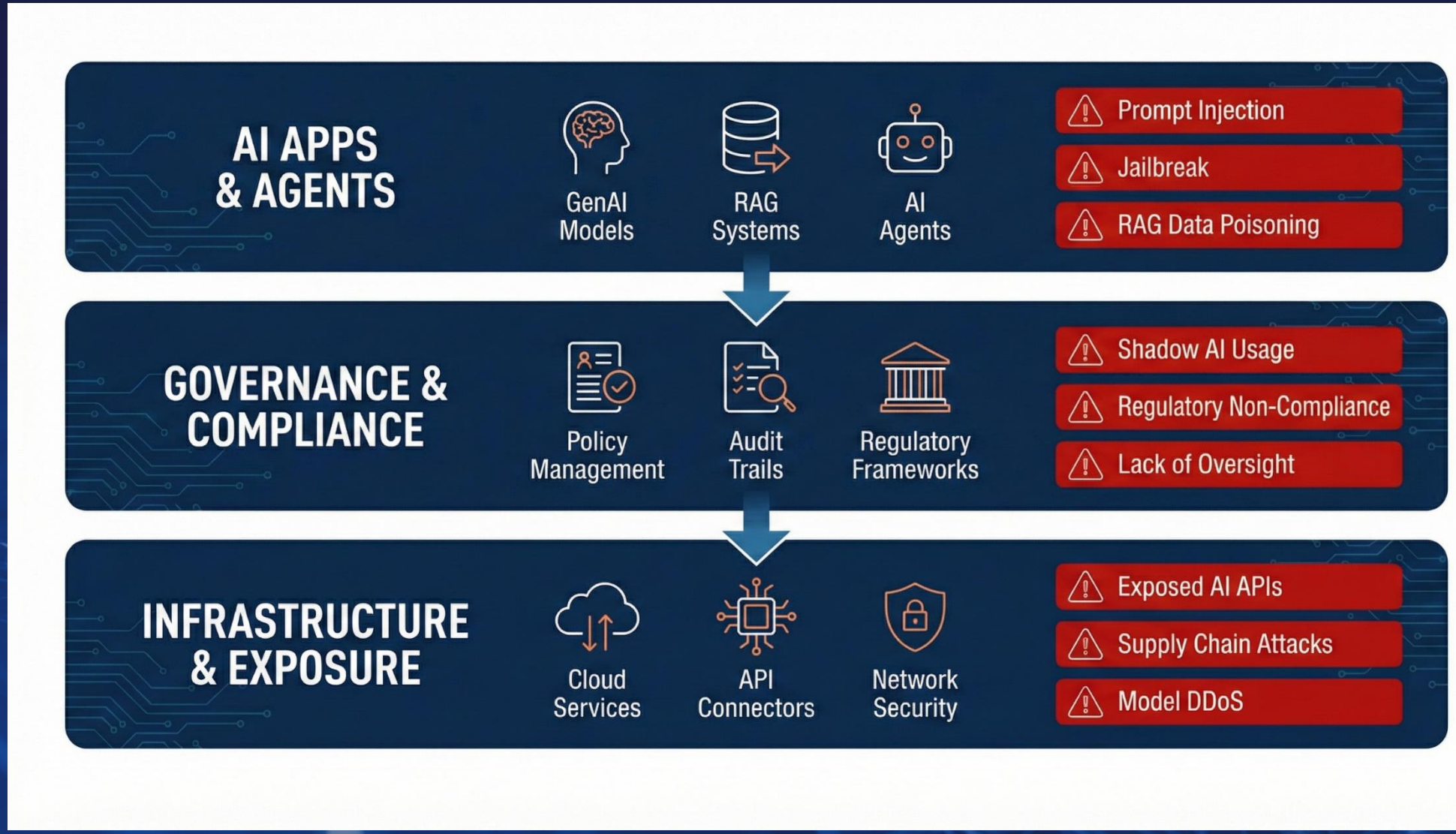
- Algoritmos de trading que colapsaron mercados en segundos.
- Chatbots que filtraron datos sensibles.
- Modelos que amplificaron sesgos a escala global.

El costo de la autonomía sin supervisión

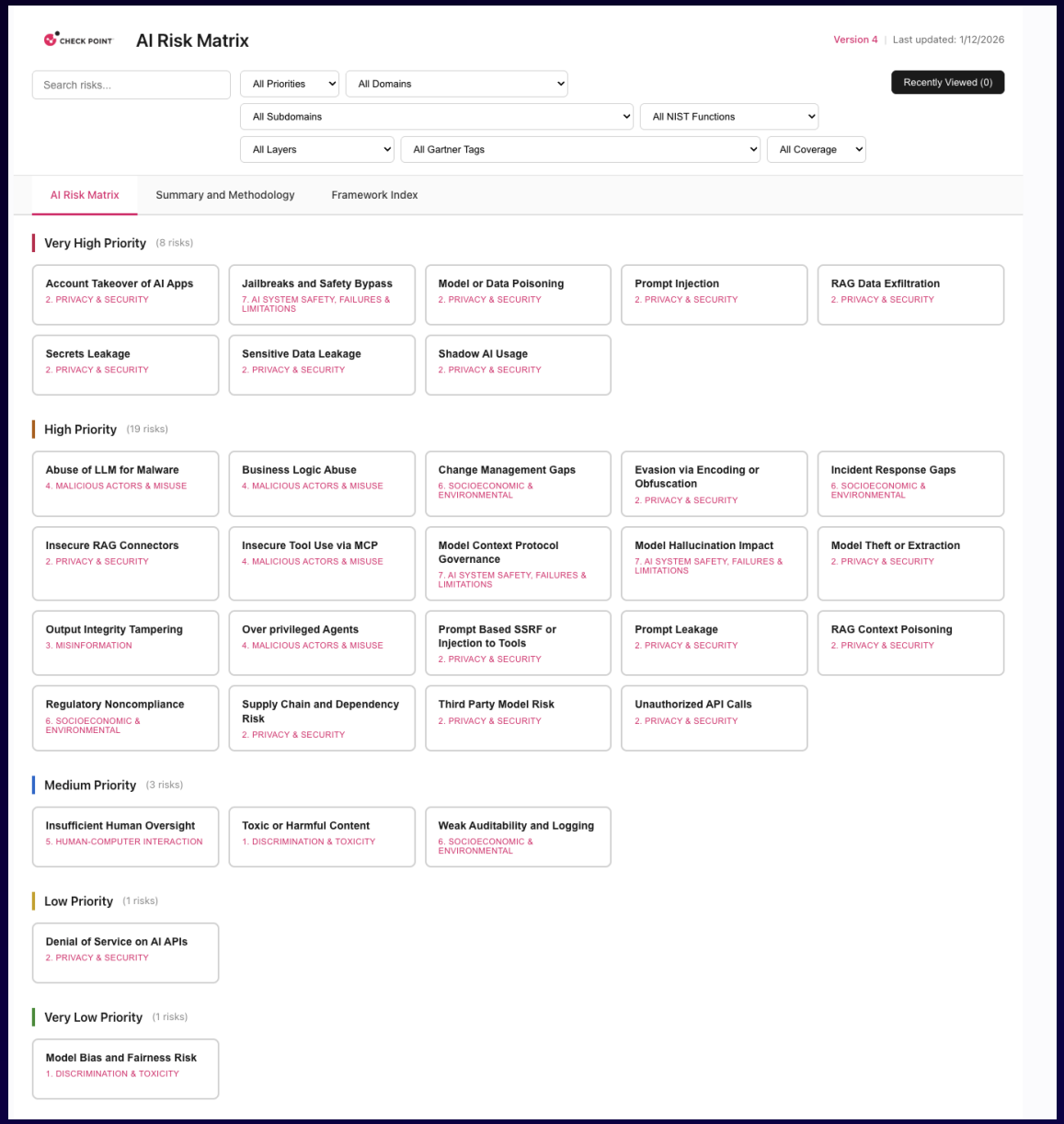
Cada incidente revela la misma verdad: sin gestión de exposición continua, la criatura supera a su creador.

El Gólem moderno no destruye con puños de arcilla, sino con decisiones automatizadas que escapan al control humano.

EL NUEVO MAPA DE RIESGOS

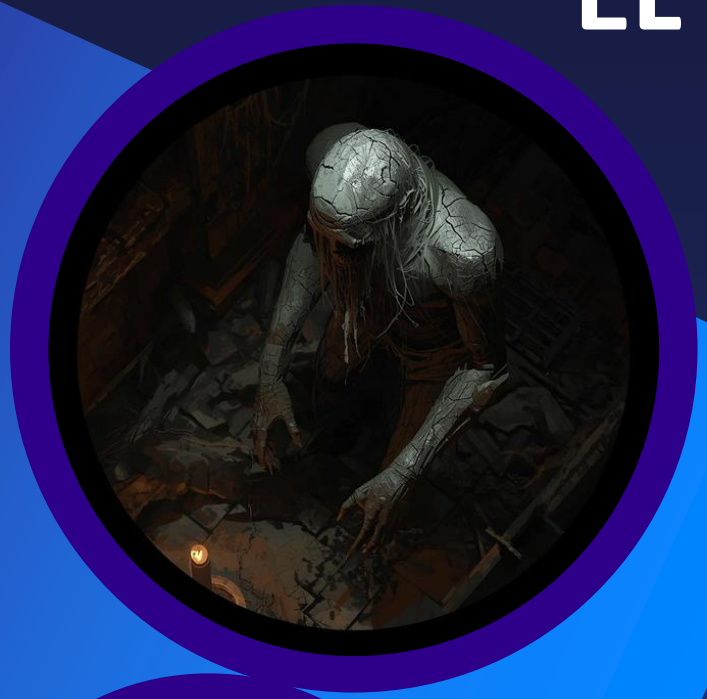


The Check Point AI Risk Matrix



- Framework-aligned AI risk map It
- Identifies 32 high-impact enterprise risks for LLMs, RAG pipelines, and agentic systems
- Maps each to MIT AI Risk Repository domains, NIST AI RMF functions, OWASP guidance, and the Gartner AI Security Platform lens

EL CAMBIO DE PARADIGMA



Seguridad Estática: El Gólem Dormido

Defensas perimetrales rígidas, evaluaciones puntuales, respuesta reactiva. Un guardián que solo despierta cuando el daño ya está hecho.

Gestión Continua: El Gólem Vigilante

Monitoreo permanente, adaptación en tiempo real, anticipación proactiva. Un protector que evoluciona con cada nueva amenaza.

LOS CUATRO PILARES DEL CONTROL

Visibilidad Total

Ver todo el panorama de exposición en tiempo real, sin puntos ciegos

Evaluación Continua

Medir y validar cada superficie de ataque de forma sistemática y constante

Priorización Estratégica

Enfocar recursos donde el impacto es mayor, alineando riesgo con valor de negocio

Remediación Activa

Actuar con precisión quirúrgica para neutralizar amenazas antes del impacto

DOMINAR AL GÓLEM:
LOS BENEFICIOS DEL CONTROL

Reducción de Riesgo Sistémico

Anticipar amenazas antes de que escalen. El Gólem controlado protege; sin control, destruye.

Cumplimiento Continuo y Resiliencia

Adaptación constante a regulaciones emergentes. Operaciones que resisten el caos digital.

EL IMPERATIVO DEL CISO

Inventario exhaustivo de IA

Mapear cada sistema de IA: modelos, datos, integraciones y puntos de exposición en toda la organización.

Evaluación continua de riesgos

Monitoreo activo de vulnerabilidades, sesgos algorítmicos y vectores de ataque emergentes.

Gobernanza adaptativa

Marcos flexibles que evolucionan con la tecnología: políticas vivas, no documentos estáticos.

LAS CUATRO VERDADES DEL GÓLEM

Crear con intención

Cada modelo de IA debe nacer con propósito definido, límites claros y controles desde el origen.

Monitorear sin pausa

La vigilancia continua no es opcional. Lo que no se observa, escapa al control.

Adaptar sin miedo

La evolución es inevitable. Los sistemas de IA deben transformarse ante nuevas amenazas sin parálisis.

Gobernar con sabiduría

El poder sin control es destrucción.
La gobernanza estratégica es el sello que da vida o muerte.

EL MOMENTO ES AHORA:
DE LA REACCIÓN A LA ANTICIPACIÓN (PREVENCIÓN)

La gestión de exposición continua en IA no es una opción futura, es una necesidad presente. Cada día sin visibilidad es un día de vulnerabilidad exponencial.

Los líderes que actúen hoy definirán los estándares de mañana. Como el Gólem, el poder de la IA requiere maestría constante para servir y no destruir.

Tomar el Control Ahora

Liderar la Transformación

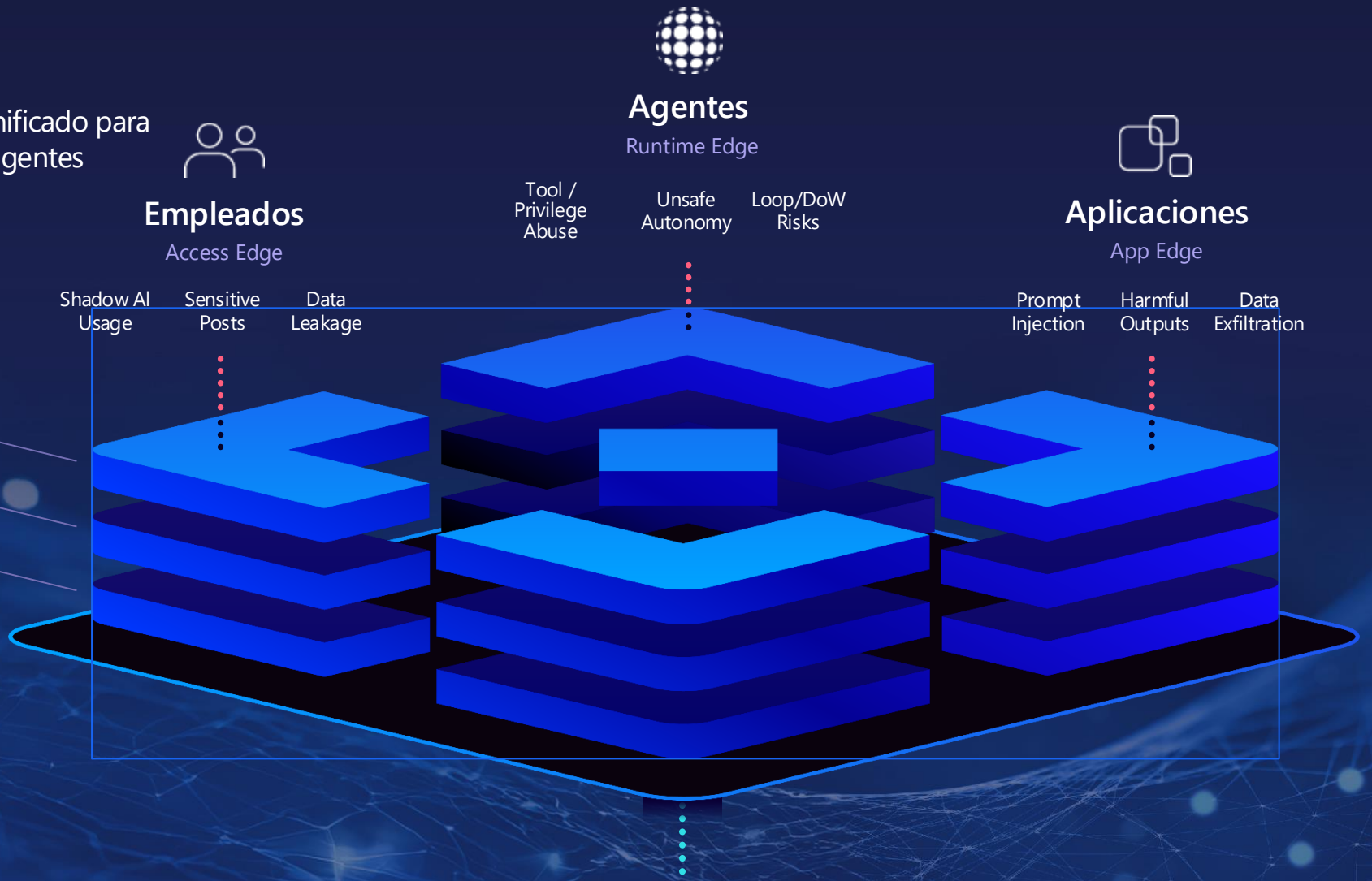
VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

CHECK POINT

EL PLANO DE DEFENSA PARA IA

Un modelo de seguridad unificado para empleados, aplicaciones y agentes



EL PLANO DE DEFENSA PARA LA IA

Una Plataforma. Una vista. Desde empleados a aplicaciones y agentes.

EL PLANO DE DEFENSA PARA IA

Una Plataforma. Una vista. Desde empleados a aplicaciones y agentes.

Workforce AI Security

Descubrimiento, gobernanza y defensa en tiempo de ejecución para el uso de IA por parte de los empleados.

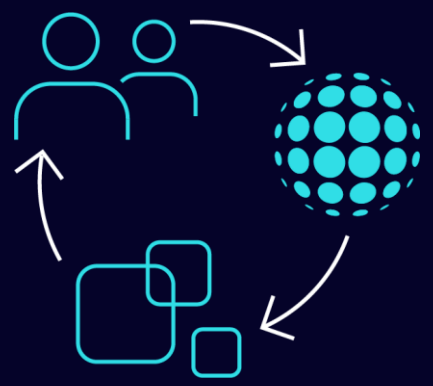
AI Agent Security

Visibilidad y protección en tiempo de ejecuciónpara aplicaciones y agentes de IA.

AI Red Teaming

Evaluaciones de amenazas basadas en riesgos y en enfoques adversariales.

Total Visibility

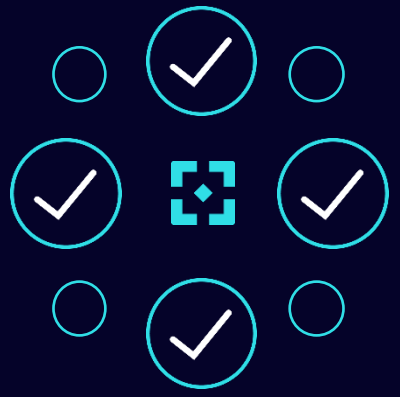


All AI usage - people, apps, agents - on one pane

Automated Protection

DLP, prompt filtering, output safety, agent control

Unified Governance



Policies, telemetry, incidents - across the entire AI lifecycle

Gandalf: The World's Largest AI Red Team

Gandalf powers Lakera with continuous adversarial insights.

- Gandalf is not just a game — it's a global adversarial AI network. Source code
- Every attack attempt feeds Lakera's threat intelligence corpus. Incident reports
- Continuous learning → stronger protection for enterprise copilots, LLMs, and Financial statements

85M+
Total prompts attempted

1M+
Players worldwide

30+ years
Of total gameplay time

VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

Gólem & IA

CHECK POINT™

MUCHAS GRACIAS !!!

Angel Salazar

asalazar@checkpoint.com