AI Security Solutions

Proteja todas as interações de IA — dos colaboradores aos agentes autônomos

A Inteligência Artificial já faz parte da operação das empresas. Colaboradores utilizam copilots, extensões, SaaS e ferramentas de GenAI diariamente. Ao mesmo tempo, aplicações corporativas passam a incorporar LLMs, agentes autônomos e integrações inteligentes capazes de executar ações diretamente em sistemas e dados críticos.

Mas a rápida adoção de IA também criou uma nova superfície de ataque. O risco agora não está apenas nos usuários ou nas aplicações tradicionais, mas nas interações entre pessoas, modelos, agentes, dados, APIs e ferramentas conectadas.

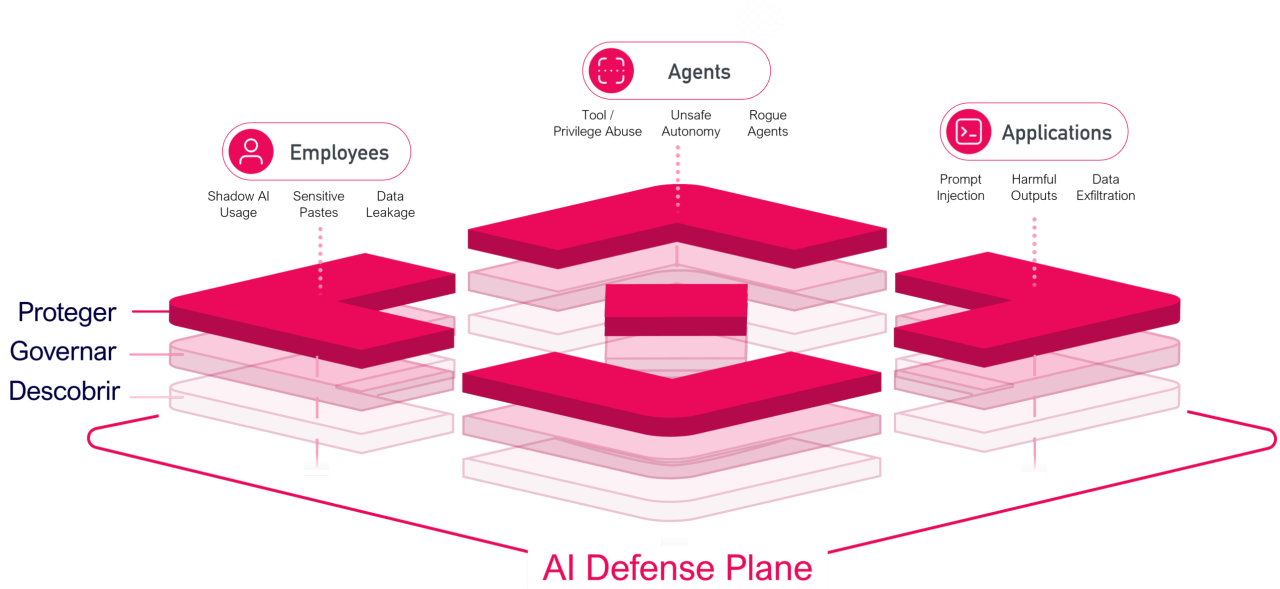
Nesse cenário, as empresas precisam enxergar e controlar riscos que antes não existiam — ou que os controles tradicionais simplesmente não conseguem interpretar, como:

- Shadow AI e falta de visibilidade sobre uso de IA
- Prompt injection, jailbreaks e instruções adversariais
- Respostas incorretas, inseguras ou não conformes
- Vazamento de dados em prompts e respostas
- Agentes executando ações inseguras ou não autorizadas
- Integrações inseguras com ferramentas, APIs, arquivos e MCPs

O problema é que controles tradicionais não foram projetados para proteger sistemas que se comunicam em linguagem natural, operam probabilisticamente, tomam decisões autônomas e interagem dinamicamente com ferramentas, APIs e arquivos.

Nesse cenário, proteger IA exige controles desenvolvidos especificamente para aplicações, agentes e interações baseadas em modelos generativos.

O PLANO DE SEGURANÇA PARA IA DA CHECK POINT



Visão geral do portfólio de AI Security da Check Point.

01 WORKFORCE AI SECURITY

Proteja o uso corporativo de IA sem comprometer produtividade.

Os colaboradores estão adotando IA mais rápido do que políticas de segurança conseguem acompanhar. Ferramentas como copilots, chatbots, extensões de navegador, IDEs com IA e SaaS com GenAI integrada já fazem parte do ambiente corporativo — muitas vezes sem visibilidade ou governança adequada.

O desafio é permitir inovação sem aumentar exposição de dados e risco operacional.

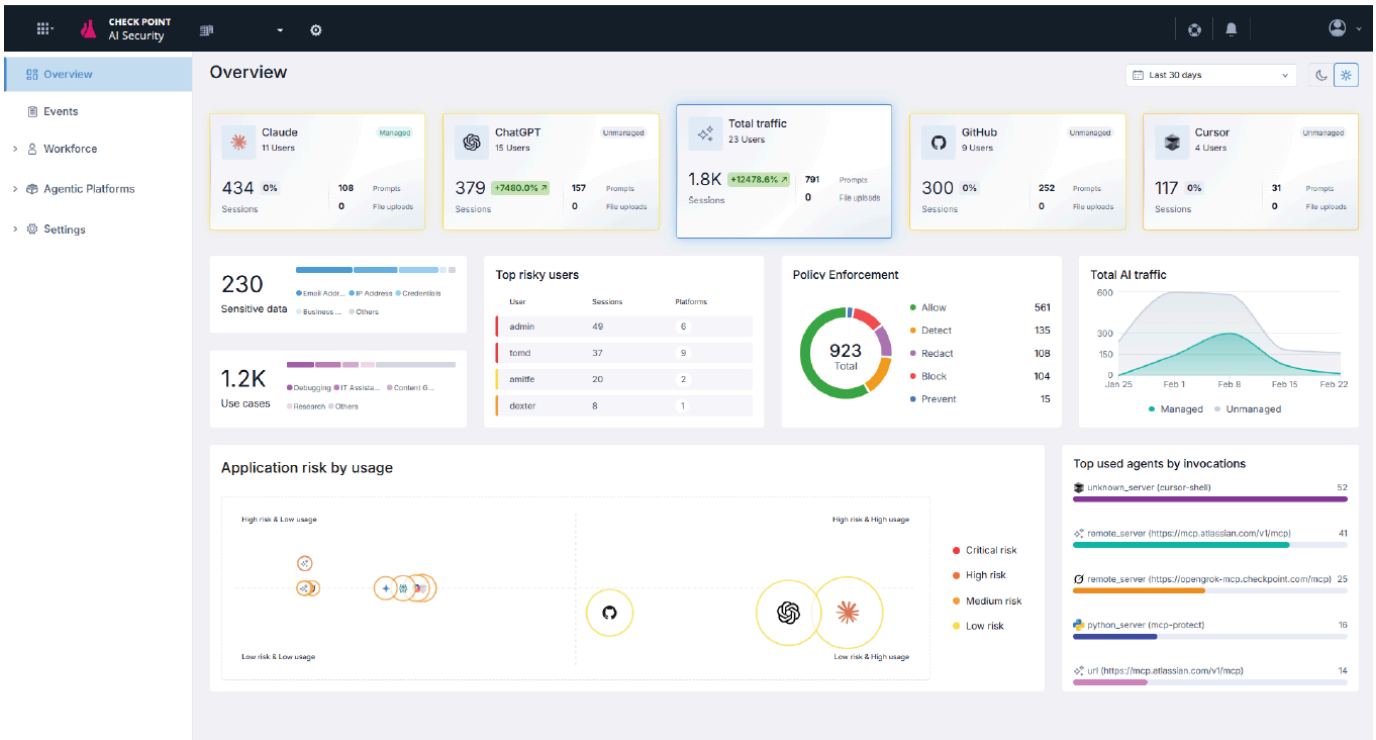
PRINCIPAIS CAPACIDADES DA PLATAFORMA

Descoberta de Shadow AI
Descubra aplicações de IA utilizadas dentro da organização — aprovadas ou não — incluindo navegadores, SaaS, extensões e ferramentas de produtividade.

Detecção de colagem de dados sensíveis
Detecte quando informações sensíveis são compartilhadas em prompts e interações com ferramentas de IA.

DLP com IA
Classifique e proteja dados sensíveis utilizando análise contextual baseada em IA, entendendo intenção e contexto conversacional.

Governança contextual
Utilize insights contextuais para definir políticas e governança sobre o uso corporativo de IA.



Exemplo visual de dashboard: visibilidade sobre aplicações, interações, riscos e uso corporativo de IA.

02 APPLICATIONS AND AGENTS SECURITY

Proteja aplicações de IA contra ataques e comportamentos não autorizados.

À medida que organizações incorporam IA em aplicações internas e customer-facing, o risco deixa de estar apenas no usuário e passa a envolver prompts, respostas do modelo, comportamento dos agentes, chamadas de ferramentas e integrações externas.

A proteção precisa acontecer inline — exatamente no momento em que prompts, respostas e ações são gerados.

Previna prompt attacks e outputs maliciosos

A solução protege aplicações contra prompt injection, jailbreaks, instruções adversariais, manipulação indireta de contexto e outputs inseguros ou não conformes.

Tudo antes que o conteúdo alcance o modelo ou o usuário.

Controle ações executadas por agentes autônomos

Agentes não apenas geram respostas — eles executam ações. À medida que agentes passam a acessar ferramentas, APIs, arquivos e sistemas corporativos, torna-se necessário controlar o que podem fazer, não apenas o que podem responder.

A plataforma intercepta chamadas de ferramentas antes da execução.

TENHA CONTROLES DE SEGURANÇA DESENVOLVIDOS ESPECIFICAMENTE PARA IA

Inspeção inline de prompts e respostas

Inspeciona prompts e respostas em tempo real para detectar prompt injection, jailbreaks, instruções maliciosas e ataques adversariais.

Proteção de dados em tempo real

Aplica proteção e redação automática de dados sensíveis em prompts e respostas sem interromper fluxos de trabalho.

Aplicação dinâmica de políticas

Permite aplicar políticas de segurança e governança em runtime, com atualização instantânea sem necessidade de redeploy.

Controle de ações de agentes

Intercepta e avalia chamadas de ferramentas realizadas por agentes antes da execução.

Inspeção de conteúdo externo e MCPs

Analisa conteúdo de APIs, arquivos, integrações externas e sistemas conectados via MCP antes que influenciem decisões do modelo.

Camada runtime agnóstica ao modelo

Opera de forma agnóstica ao modelo, suportando cloud, on-premises, ambientes híbridos e múltiplos providers de IA.

CG ONE + CHECK POINT: SEGURANÇA PARA A NOVA ERA DA IA

CG One + CHECK POINT

IA com governança, visibilidade e proteção

A CG One apoia organizações na construção de estratégias de AI Security que vão além da proteção tradicional de usuários e aplicações.
Em parceria com a Check Point, nossa parceira há mais de 30 anos, ajudamos empresas a obter visibilidade, governança e proteção para colaboradores, aplicações baseadas em IA e agentes autônomos — permitindo inovação sem abrir mão de segurança e compliance.

Entre em contato e saiba mais.
cg-one.com

Entre em contato →