Visão geral da Zscaler AI Security

VISÃO GERAL

Benefícios da segurança de IA

DESCUBRA OS ATIVOS E RISCOS DE IA
Descubra e mapeie todo o seu ecossistema de IA, desde IA paralela e aplicativos de risco até modelos e fluxos de trabalho de IA, entre outros.

ENCONTRE VULNERABILIDADES DE IA
Faça testes de red team dos sistemas de IA para identificar vulnerabilidades e riscos com testes contínuos e automatizados.

PROTEJA O ACESSO À IA
Utilize mecanismos de proteção de IA inline para aplicar proteções em tempo real contra ameaças, perda de dados e uso seguro.

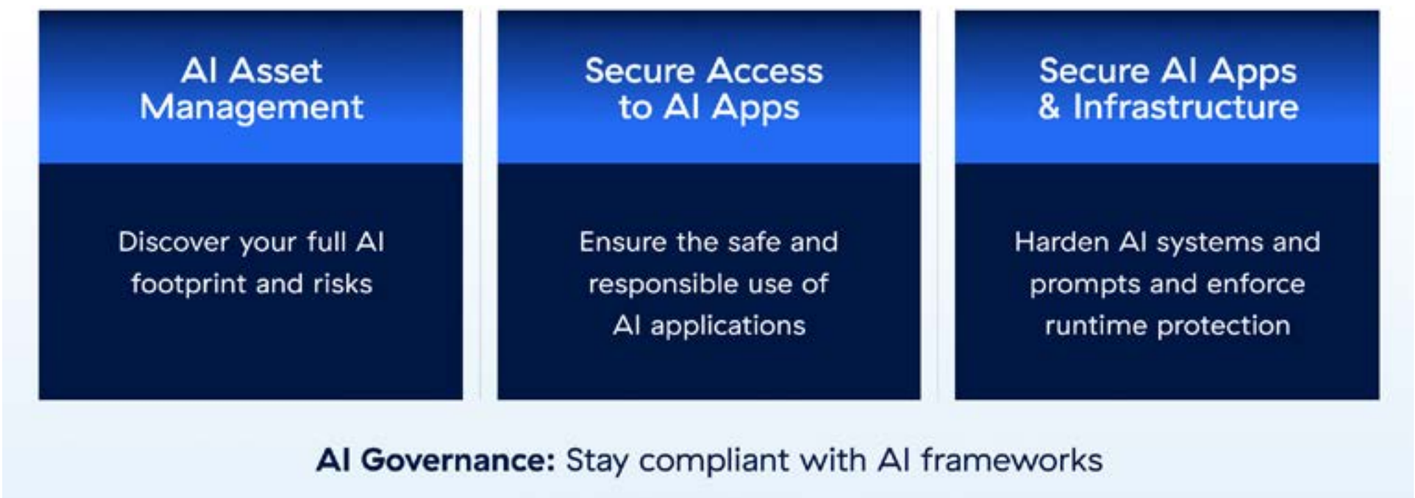
ADMINISTRE A CONFORMIDADE DE IA
Gerencie sua presença e implantações de IA usando estruturas de IA para manter a conformidade de riscos

Segurança de IA de ponta a ponta com a Zscaler

A Zscaler oferece soluções baseadas em IA, projetadas para ajudar as empresas a aproveitar o poder transformador da IA, ao mesmo tempo em que gerenciam os riscos associados.

Com funcionalidades que vão desde a identificação de usos de risco da IA até a garantia de desenvolvimento seguro e a proteção de versões sigilosas por meio de defesas inline avançadas.

A Zscaler redefine o significado de proteger a inovação em IA. Desbloqueie o potencial da IA com confiança e promova o progresso sem medo com a Zscaler.



Por que escolher a Zscaler para segurança de IA

CICLO DE VIDA COMPLETO DA IA
Segurança de IA: da descoberta à implementação

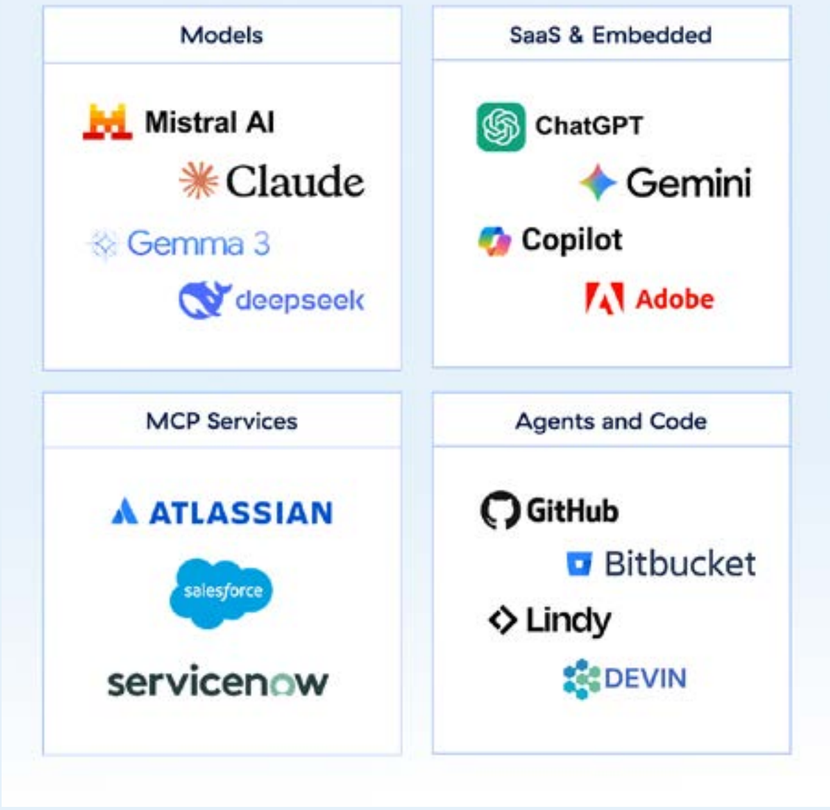
PLATAFORMA UNIFICADA
Plataforma comprovada que integra segurança de IA com zero trust

PARCEIRO COMPROVADO
Especialização em sucesso do cliente e transformação

Descoberta de ativos com AI-SPM

Descobrir sua presença de IA é um desafio no ambiente de IA dinâmico de hoje. Sem uma visibilidade clara da IA paralela, dos modelos, serviços, servidores de MCP e pipelines, as organizações têm dificuldade em detectar e responder aos riscos de forma eficaz.

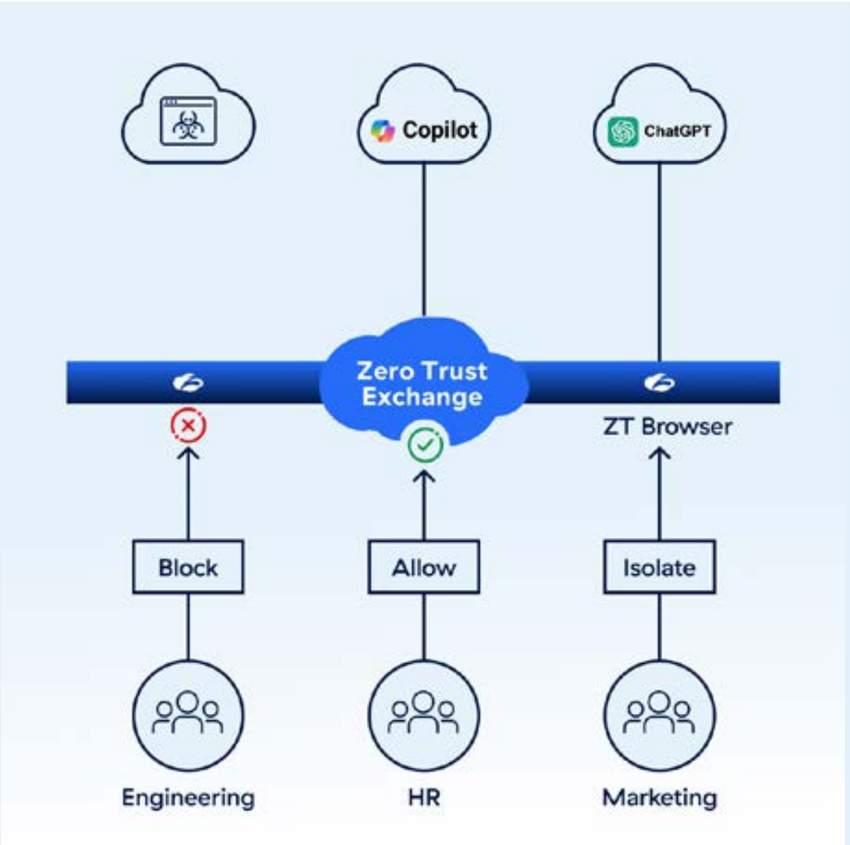
Com o Zscaler AI SPM, as organizações obtêm visibilidade abrangente de seus ecossistemas de IA. Ele fornece informações sobre sua presença em aplicativos de GenAI, LLMs, modelos, servidores de MCP e pipelines, ajudando você a identificar exposições e vulnerabilidades de risco que podem comprometer seus dados e negócios.



Segurança de acesso de IA

Controlar o acesso e garantir a segurança dos aplicativos SaaS de GenAI está se tornando um desafio cada vez maior. Com a IA paralela se espalhando sem controle e os riscos crescentes de perda de dados ou uso não conforme, as organizações precisam de soluções eficazes para lidar com essas ameaças.

Com a segurança de acesso de IA da Zscaler, você pode garantir o uso seguro, em conformidade com as normas e responsável de aplicativos de IA. Aplique controles de acesso granulares para determinar quais usuários ou aplicativos podem interagir com ferramentas de IA. Utilize a proteção ou o isolamento de DLP para evitar a perda de dados por meio de prompts e aplique a moderação de conteúdo para garantir a conformidade com as políticas de uso aceitável da empresa.



©2026 Zscaler, Inc. Todos os direitos reservados.

Testes com red teaming automatizado

Testar sistemas de IA em busca de vulnerabilidades costuma ser um processo complexo e demorado. Para organizações sem recursos de red team dedicados, pode parecer quase impossível realizar avaliações completas.

A solução de red teaming automático e contínuo da Zscaler aborda esses desafios com um mecanismo inovador e automatizado de simulação de ataques. Com mais de 25 categorias de teste predefinidas e suporte para categorias totalmente personalizadas e uploads de conjuntos de dados, o SPLX permite que as organizações adaptem os cenários de teste aos seus domínios, ambientes regulatórios e casos de uso específicos.



Proteção inline com AI Guard

Os LLMs rapidamente se tornaram um novo e perigoso vetor de ameaças e perda de dados. Sem uma inspeção inline de alto desempenho dessas conexões, as organizações ficam vulneráveis à exposição de dados, sistemas de IA comprometidos e ameaças maliciosas.

Com o Zscaler AI Guard, as organizações podem fornecer inspeção inline de alto desempenho para prompts e interações de IA. Detecte ameaças de risco, como injeções de prompt e desbloqueio de dispositivos (jailbreaking), previna a perda de dados sigilosos e modere o conteúdo para garantir o uso seguro e as políticas de uso aceitável. Com base na experiência de um líder reconhecido em inspeção inline, a Zscaler garante proteção robusta para seu tráfego crítico de IA.

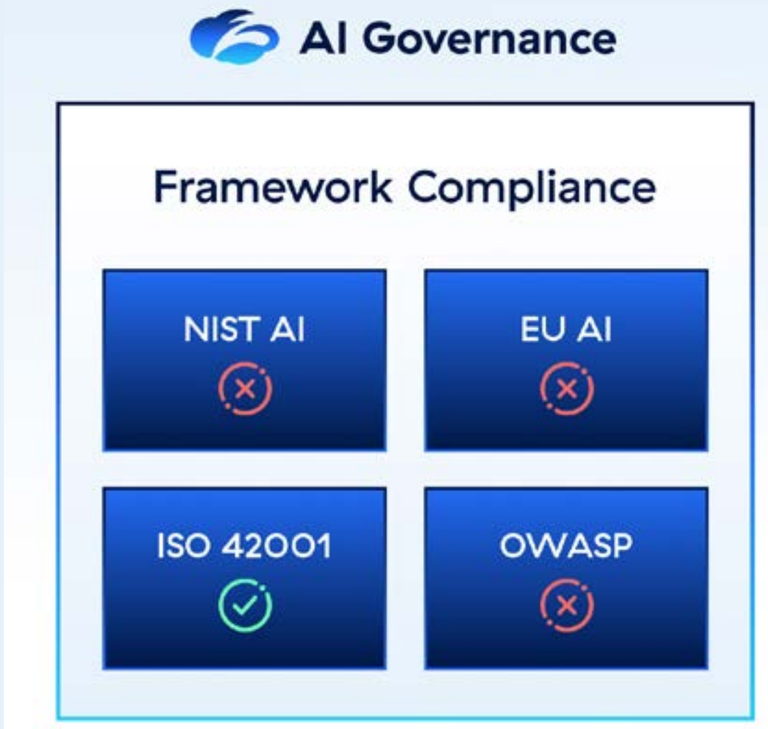


©2026 Zscaler, Inc. Todos os direitos reservados.

Governança de IA com AI SPM

Garantir a conformidade e a governança dos sistemas de IA está se tornando cada vez mais complexo à medida que as organizações adotam a IA em larga escala. Sem a devida supervisão do cumprimento de políticas e dos frameworks de IA, as empresas ficam expostas a riscos legais, financeiros e reputacionais.

Com a abordagem da Zscaler para governança de IA, você pode automatizar o monitoramento da conformidade e simplificar os processos de geração de relatórios. Monitore continuamente os sistemas de IA para garantir a conformidade com as políticas internas e os padrões regulatórios, fornecendo as evidências necessárias para dar suporte a auditorias e atender aos requisitos. Garanta que o uso da IA esteja em conformidade com as estruturas de governança, ajudando sua organização a mitigar riscos e manter a integridade operacional.



Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange™ protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange™ baseada em SSE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.

© 2026 Zscaler, Inc. Todos os direitos reservados. Zscaler™ e outras marcas registradas listadas em **zscaler.com/legal/trademarks** são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.

+1 408.533.0288 **Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/br**

zscaler™

Zero Trust Everywhere