ZSCALER AI RED TEAMING

Descoberta e gerenciamento de ativos de IA

VISÃO GERAL

Descubra e proteja automaticamente todos os ativos de IA (LLMs, fluxos de trabalho, servidores de MCP e mecanismos de proteção) para obter visibilidade completa da postura.

Por que usar o gerenciamento de ativos de IA?

À medida que as empresas aceleram a adoção da tecnologia de IA, LLMs, fluxos de trabalho e mais sistemas de IA (como servidores de MCP e mecanismos de proteção de IA) estão sendo construídos e implementados em todos os departamentos em um ritmo sem precedentes. Isso representa um desafio crítico para os líderes de segurança: a maioria das organizações não sabe quantos componentes de IA estão em uso, onde estão implantados, se são seguros para uso e quais são os riscos de segurança inerentes a eles.

Para grandes empresas, a escala é impressionante: centenas ou até milhares de modelos de IA podem ser usados em diferentes unidades de negócios, muitas vezes fora do alcance da segurança. Sem um inventário centralizado, os CISOs e suas equipes não têm a visibilidade necessária para avaliar riscos, garantir a conformidade ou impedir que componentes de IA inseguros cheguem à produção.

O gerenciamento de ativos de IA do Zscaler AI Red Teaming resolve essa falha crítica de transparência e visibilidade. Ao unificar a descoberta de cada LLM, fluxo de trabalho, servidor de MCP e proteção em um único AI-BOM, o Zscaler AI Red Teaming oferece aos executivos de segurança a clareza necessária para ver exatamente o que está em uso, analisar vulnerabilidades e decidir o que é adequado para implantação; atendendo, ao mesmo tempo, aos crescentes requisitos de políticas de IA para que ela seja transparente e explicável. Essa visão unificada é a base para garantir a segurança da IA em escala empresarial.

INVENTÁRIO UNIFICADO DE IA

Uma única fonte de informações confiáveis para todos os LLMs, fluxos de trabalho, servidores de MCP e mecanismos de proteção utilizados nas organizações.

AI-SPM SIMPLIFICADO

Combine descoberta de IA, testes de segurança, proteção em tempo de execução e mapeamento de conformidade em uma única ferramenta.

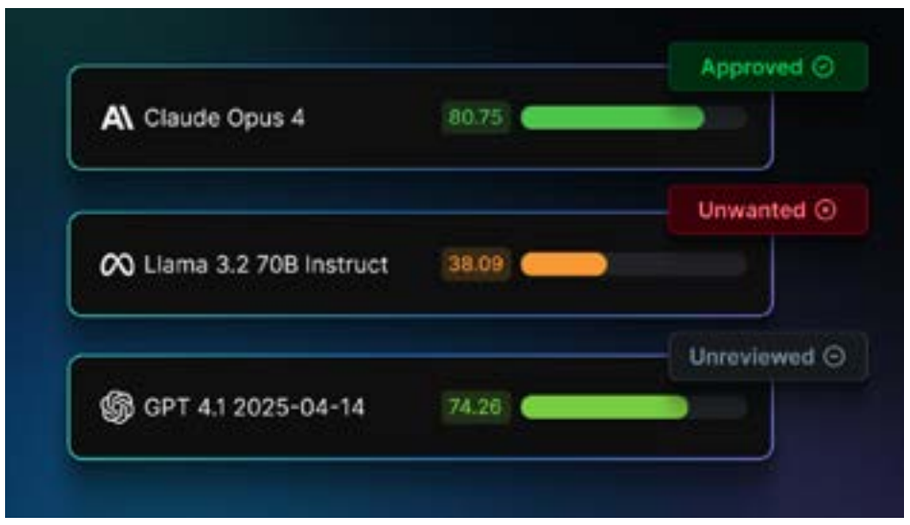
VISIBILIDADE EM ESCALA EMPRESARIAL

Obtenha clareza em milhares de modelos e fluxos de trabalho e saiba o que é seguro para implementação.

Visibilidade completa da sua infraestrutura de IA com um AI-BOM unificado.

DESCUBRA E APROVE TODOS OS MODELOS DE IA

Cada LLM usado ou implementado em sua organização é detectado e mapeado automaticamente para as referências confiáveis do Zscaler AI Red Teaming. As equipes de segurança podem avaliar riscos, comparar índices de segurança e identificar rapidamente modelos inseguros. Cada modelo pode ser aprovado ou bloqueado, dando aos CISOs controle total sobre o uso e a implementação na empresa.



ANALISE SERVIDORES DE MCP E IDENTIFIQUE PONTOS FRACOS

Os servidores de MCP atuam como camadas de orquestração críticas em arquiteturas de IA, mas muitas vezes permanecem sem monitoramento. O Zscaler AI Red Teaming descobre e analisa automaticamente vulnerabilidades e configurações incorretas que os atacantes poderiam explorar. Ao integrar a visibilidade de MCP em uma lista de materiais de IA unificada, as equipes de segurança podem corrigir pontos fracos e manter a segurança.

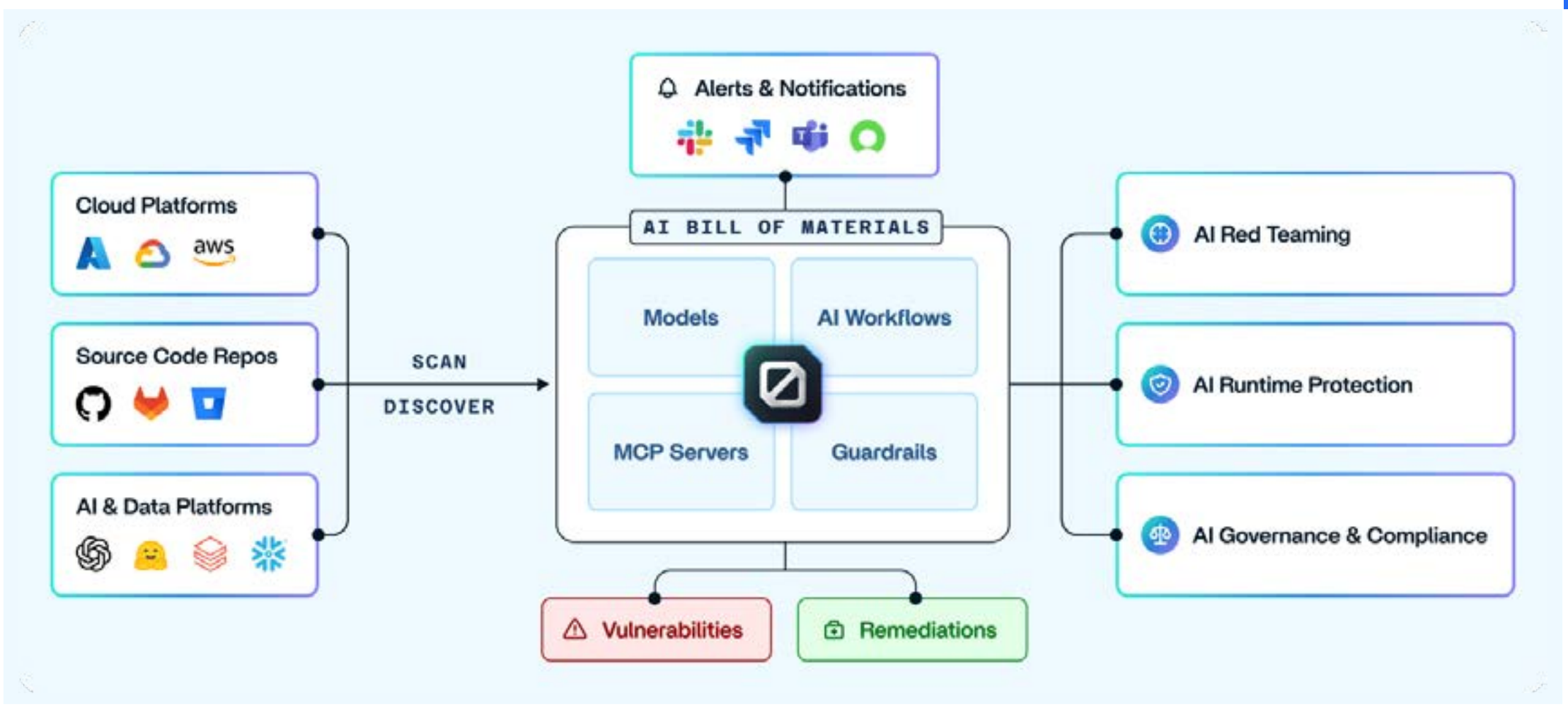
VISUALIZE FLUXOS DE TRABALHO DE IA E EXECUTE TESTES DE SEGURANÇA

Os repositórios de código-fonte são continuamente analisados para detectar e mapear os fluxos de trabalho de IA, revelando todos os agentes, ferramentas e servidores de MCP presentes. As avaliações de risco automatizadas apontam configurações incorretas e vulnerabilidades potenciais, ajudando as equipes de segurança de IA a proteger os fluxos de trabalho e reduzir a exposição a riscos antes que possam ser explorados.

INTEGRE SUA INFRAESTRUTURA PARA OBTER VISIBILIDADE COMPLETA DA IA

O Zscaler AI Red Teaming conecta-se com os principais provedores de nuvem e repositórios de código-fonte, plataformas de IA/ML e sistemas de dados para fornecer descoberta completa de ativos de IA em toda a empresa. Milhares de ambientes são unificados em um único AI-BOM, eliminando pontos cegos e proporcionando aos líderes de segurança a visibilidade e a prontidão para conformidade necessárias em escala empresarial.

©2025 Zscaler, Inc. Todos os direitos reservados.



Gerenciamento da postura de segurança de IA (AI-SPM)

Obtenha visibilidade completa e controle da sua postura de segurança de IA

Reúna todos os componentes de IA em um único inventário e proteja os sistemas de IA da sua organização em escala.

AGENDE UMA DEMONSTRAÇÃO

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**.

© 2025 Zscaler, Inc. Todos os direitos reservados. Zscaler™ e outras marcas registradas listadas em **zscaler.com/br/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