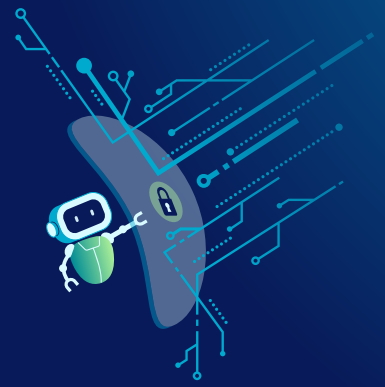
netskope

o checklist de segurança em IA

Um guia prático para CISOs e equipes de segurança sobre como proteger o uso de IA

o checklist de segurança em IA



As empresas estão adotando a IA rapidamente, pressionando as equipes de segurança a garantir que tenham as bases corretas para implantá-la com segurança. Mas, na corrida para aproveitar os benefícios da IA, é vital que as organizações não percam nenhum passo.

Este checklist apresenta as perguntas mais importantes que você precisa fazer ao examinar seu ambiente, políticas e controles. Ele foi projetado para ajudar os líderes de segurança a avaliar rapidamente o status atual e identificar os próximos passos, facilitando a identificação de lacunas, a priorização de ações e aumentando a confiança sobre onde concentrar os esforços.

Descobrir

Identifique toda a utilização de IA em toda a organização

Houve uma explosão de ferramentas de IA nas empresas recentemente, e nem tudo isso é evidente para os profissionais de segurança. O uso de shadow AI continua sendo um problema persistente: 47% dos usuários de IA ainda utilizam aplicativos pessoais de IA no trabalho (Netskope, 2026 Cloud and Threat Report). Existe também a possibilidade de que seu portfólio atual de aplicativos SaaS possa adicionar recursos de IA que aumentem o risco de dados. As equipes de segurança precisam analisar minuciosamente cada ferramenta quanto ao seu impacto em IA.

Considerar

Temos visibilidade tanto das ferramentas de IA gerenciadas quanto das não gerenciadas?

É possível identificar funcionalidades de IA incorporadas em aplicativos SaaS?

Compreendemos como os usuários e agentes interagem com os modelos de IA atualmente?

Analisar

Entenda sua exposição de dados relacionada à IA e os padrões de risco

Nem todos os dados têm o mesmo valor. Esse princípio tem orientado as políticas de segurança corporativa há muito tempo. Mas isso nunca foi tão importante quanto na era da IA, quando as equipes de segurança estão tentando encontrar o equilíbrio certo entre acelerar a inovação e controlar os riscos. Uma compreensão mais detalhada de como as ferramentas de IA estão sendo usadas e que tipo de dados estão fluindo por elas pode ajudar as organizações a tomar decisões mais inteligentes e a concentrar seus recursos de forma mais eficaz.

Considerar

Sabemos que tipos de dados estão sendo compartilhados com as ferramentas de IA?

É possível distinguir entre interações de IA de baixo e alto risco?

Somos capazes de identificar padrões que indiquem riscos emergentes?

Aplicar

Aplique controles de uso seguro em todas as interações de IA

No cerne da abordagem zero trust para segurança está a compreensão de que as necessidades de acesso são contextuais. Conceder o acesso apropriado torna-se mais complicado com a IA, quando as ferramentas podem inadvertidamente fornecer informações confidenciais a um colega que consulta uma ferramenta de IA corporativa. A essa complexidade soma-se a implantação contínua de agentes de IA, que introduzem novos vetores de ataque, incluindo ações autônomas inseguras e vias ampliadas para exfiltração de dados.

Considerar

Podemos controlar o uso da IA e o acesso aos dados com base na identidade do usuário/agente, na sensibilidade dos dados ou no risco?

Os controles são consistentes em diferentes ferramentas e ambientes de IA?

Nossos modelos privados de IA estão protegidos contra tentativas de jailbreaking ou de engenharia de prompts maliciosa?

Governar

Garanta que a utilização da IA esteja em conformidade com as normas, seja rastreável e gerida de forma responsável

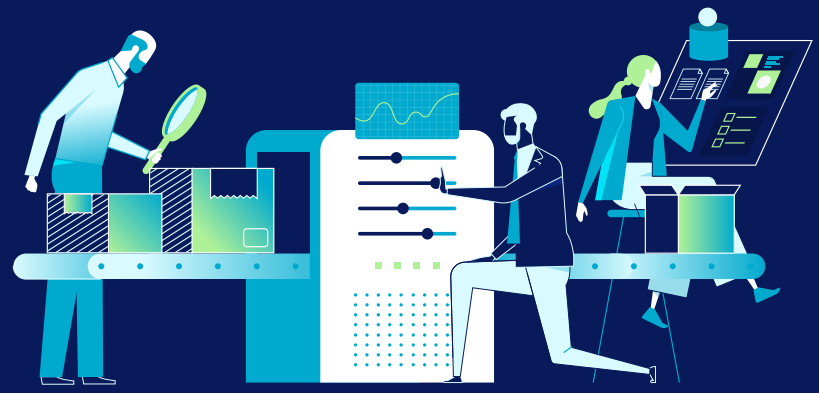
Os profissionais de segurança sabem que a conformidade com os padrões do setor é essencial. Mas as regulamentações de IA estão em constante evolução para acompanhar a tecnologia, por isso é importante adaptar as políticas de segurança de acordo e manter registros de auditoria claros em todos os momentos. Isso é particularmente imperativo em setores como serviços financeiros e saúde, onde a regulamentação é fundamental para os negócios.

Considerar

Podemos demonstrar como o uso da IA é governado atualmente?

Temos capacidade de auditoria e rastreabilidade em todas as interações de IA?

As responsabilidades pelo uso da IA estão claramente definidas?



Pronto para descobrir mais? Saiba mais sobre a abordagem da Netskope para proteger a IA aqui.

Sobre a Netskope

A Netskope, líder em segurança e redes modernas para a era da nuvem e da IA, atende às necessidades das equipes de segurança e de redes, oferecendo acesso otimizado e segurança em tempo real, com base em contexto, para pessoas, dispositivos e dados onde quer que estejam. Milhares de clientes, incluindo mais de 30% das empresas da Fortune 100, confiam na plataforma Netskope One, em seu Zero Trust Engine e na poderosa rede NewEdge para reduzir riscos e obter total visibilidade e controle sobre aplicações na nuvem, IA, SaaS, web e privadas — oferecendo segurança e acelerando o desempenho sem sacrifícios.

netskope

Interessado em saber mais?

Peça uma demonstração