Configurar o DLP para proteger dados confidenciais de serem usados pelo ChatGPT

Contents

Introdução

Este documento descreve como usar a Prevenção de Perda de Dados (DLP - Data Loss Prevention) para proteger dados confidenciais de serem usados pelo ChatGPT.

Overview

O mundo da inteligência artificial está fervilhando, com inovações como o modelo de linguagem da OpenAI, ChatGPT, liderando o ataque. Essa força da IA vem crescendo em um ritmo alucinante, transformando vários setores com suas conversas inteligentes e sensíveis ao contexto. No entanto, com esses grandes avanços, surgem alguns desafios em potencial, especificamente os riscos de perda de dados.

Pense no ChatGPT como um parceiro de conversa super inteligente que gera texto com base no que você alimenta. Agora, se houver informações confidenciais na combinação e elas não forem tratadas corretamente, haverá um risco de violações de dados. Isso destaca por que é tão importante ter um plano abrangente de Prevenção de Perda de Dados (DLP) em vigor.

Sua solução Umbrella DLP foi projetada para proteger sua empresa contra esses riscos. Aqui estão três casos de uso urgentes que nossa solução pode ajudá-lo a solucionar imediatamente e que levam apenas cerca de 5 minutos para serem implementados.

A. Conformidade com as regulamentações de privacidade de dados, como GDPR, HIPPA e PCI-DSS:

1. Vá para Policies > Management > Data Loss Prevention Policy no painel do seu Umbrella.
2. Comece a criar uma nova regra PPD. Basta clicar em Adicionar regra no lado superior direito e selecionar Regra em tempo real.
3. Dê à sua regra um nome que seja fácil de reconhecer, como "ChatGPT Protection", e escolha o nível de gravidade (de Baixo a Crítico) que atenda às suas necessidades.
4. Na seção Classificações, selecione uma ou mais das Classificações de Conformidade Internas relevantes para sua organização. Pode ser, por exemplo, a "Classificação GDPR integrada" ou a "Classificação PCI integrada".
5. Na seção Identidades, selecione todas as identidades que deseja monitorar e proteger. Se possível, recomendamos uma ampla seleção para uma cobertura

abrangente.

6. Vá para a seção Destinos, selecione Listas de destino e aplicativos para inclusão e escolha OpenAI ChatGPT.
7. Agora é tempo de agir. Na seção Ação, você pode escolher Monitorar ou Bloquear. Se você for novo nisso, recomendamos começar com a ação 'Monitorar'. Isso permite que você observe os padrões de uso e tome uma decisão mais informada sobre os possíveis riscos e benefícios.
8. Se você tiver escolhido a ação 'Monitorar', verifique o relatório PPD após uma semana ou um mês. Isso mostra quem está compartilhando informações confidenciais com o ChatGPT e quando, ajudando você a decidir se uma ação de 'Bloquear' é necessária.

B. Proteção de informações de identificação pessoal (PII): Para proteger o PII em sua organização contra os riscos do ChatGPT, basta usar as mesmas instruções acima, mas na etapa 4, selecione a 'Classificação PII Interna' em vez das classificações de conformidade.

C. Proteção do código fonte e da propriedade intelectual: Se a sua organização usa ChatGPT para atividades que envolvem código-fonte ou outra propriedade intelectual, siga estas etapas:

1. Primeiro, crie uma nova classificação de dados do código-fonte. Navegue até Policies > Management > Policy Components > Data Classification. Clique no botão Add no lado superior direito e dê à sua classificação de dados um nome reconhecível, como 'Source Code Classification'.
2. Escolha Código-fonte na lista de Identificadores de dados internos.
3. Click Save.
4. Depois de salvar, revise as instruções de 'Conformidade com os regulamentos de privacidade de dados' acima, mas na etapa 4, escolha a Classificação de dados do código-fonte recém-criada em vez das internas.

O processo é simples e leva apenas alguns minutos do seu tempo, mas os benefícios para a segurança e a conformidade da sua empresa são inestimáveis. Exortamos você a tomar essas medidas o mais rápido possível para fortalecer sua proteção de dados.

Quer saber mais sobre os riscos de IA geradora e como a Umbrella pode protegê-lo, assista ao webinar Proteja seus dados confidenciais do uso do ChatGPT.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.