Configurar o suporte DLP e CASB para AI e ChatGPT geradores

Contents

Introdução

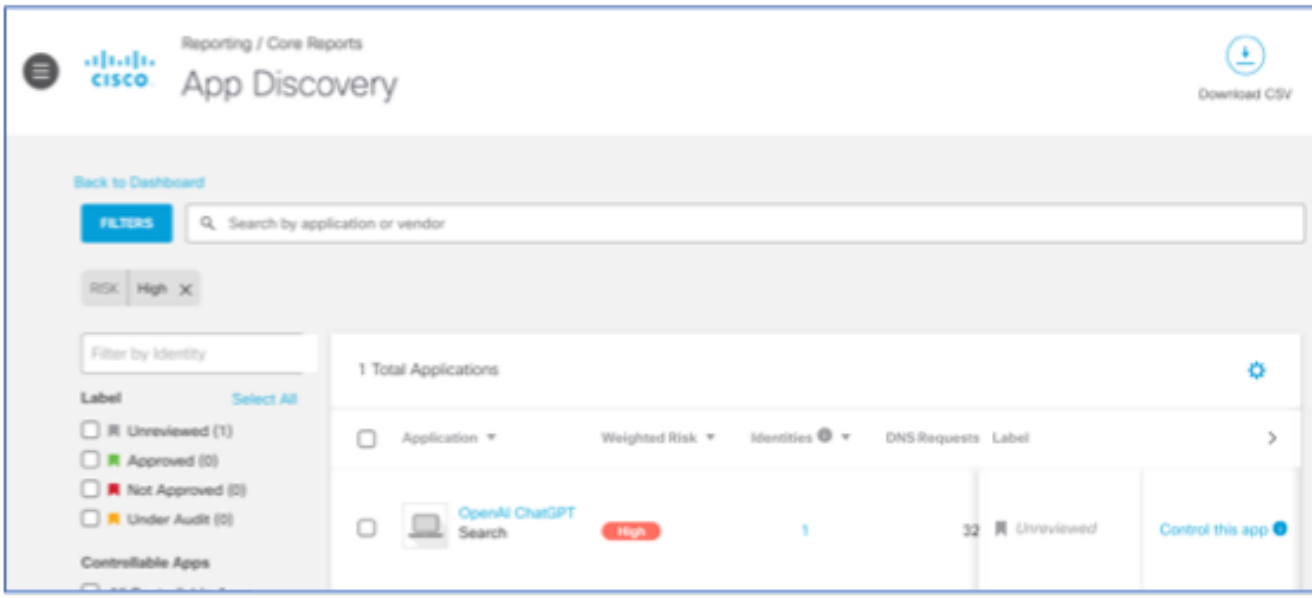
Este documento descreve o Cloud Access Security Broker (CASB) e o suporte à Prevenção de Perda de Dados (DLP) para IA Gerativa e ChatGPT.

Overview

Lançamos novos aprimoramentos do Cloud Access Security Broker (CASB) e do Data Loss Prevention (DLP) no nosso pacote de produtos do Umbrella , projetado para ajudar os clientes a gerenciar o uso do ChatGPT em suas organizações de forma mais eficaz.
Essas melhorias permitem que nossos clientes garantam que seus funcionários estejam usando o ChatGPT com responsabilidade e segurança, ao mesmo tempo em que protegem informações confidenciais de riscos em potencial.

Estes são os principais recursos:

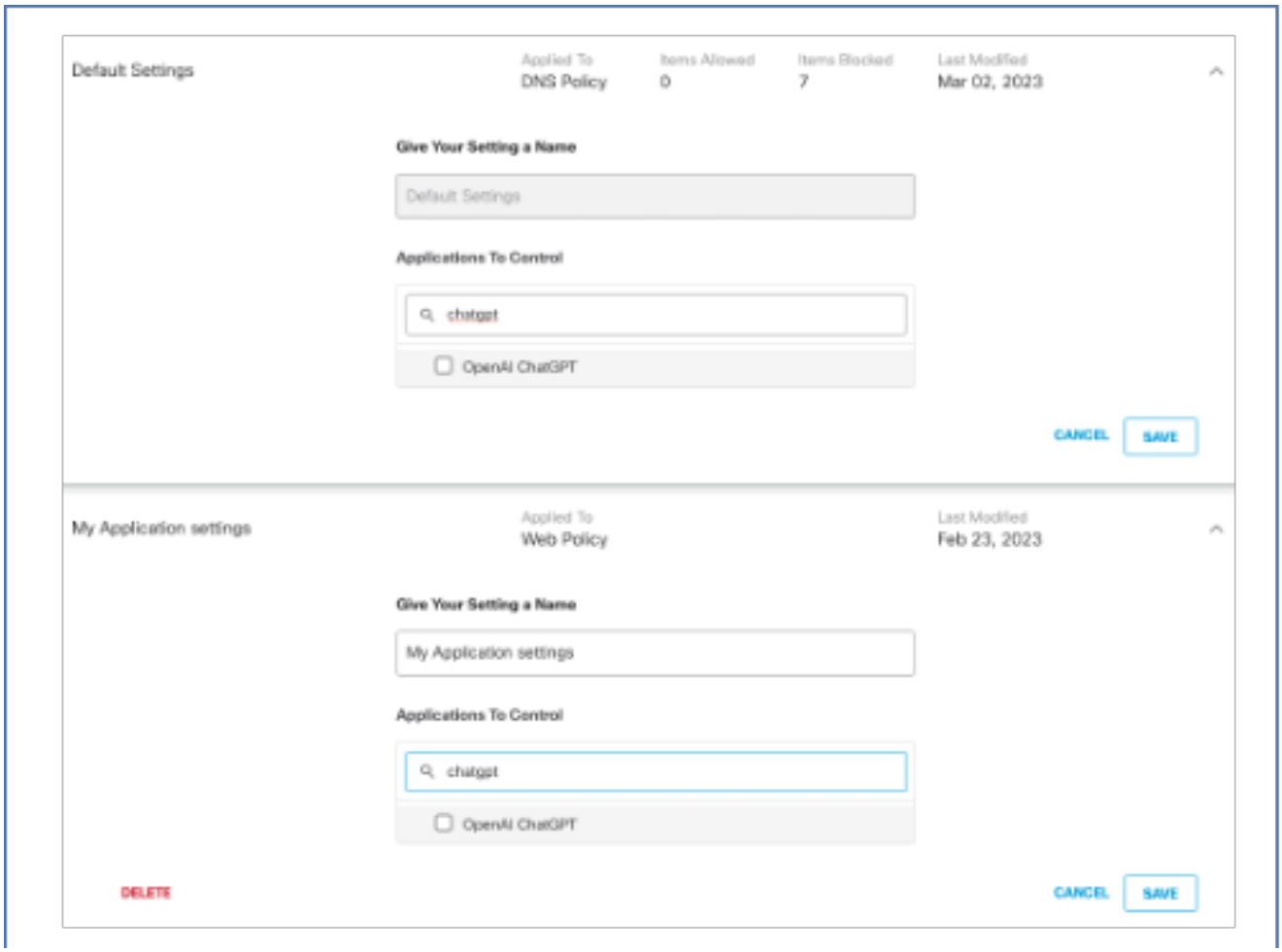
1. Descobrindo o uso de ChatGPT na organização:
   Usando o relatório App Discovery (Relatórios -> Relatórios principais), os clientes podem identificar e monitorar o uso de ChatGPT em sua organização.
   Isso fornece informações valiosas sobre como os funcionários estão usando a ferramenta, permitindo que eles otimizem seu uso e garantam a conformidade com suas políticas internas.



16221272854164

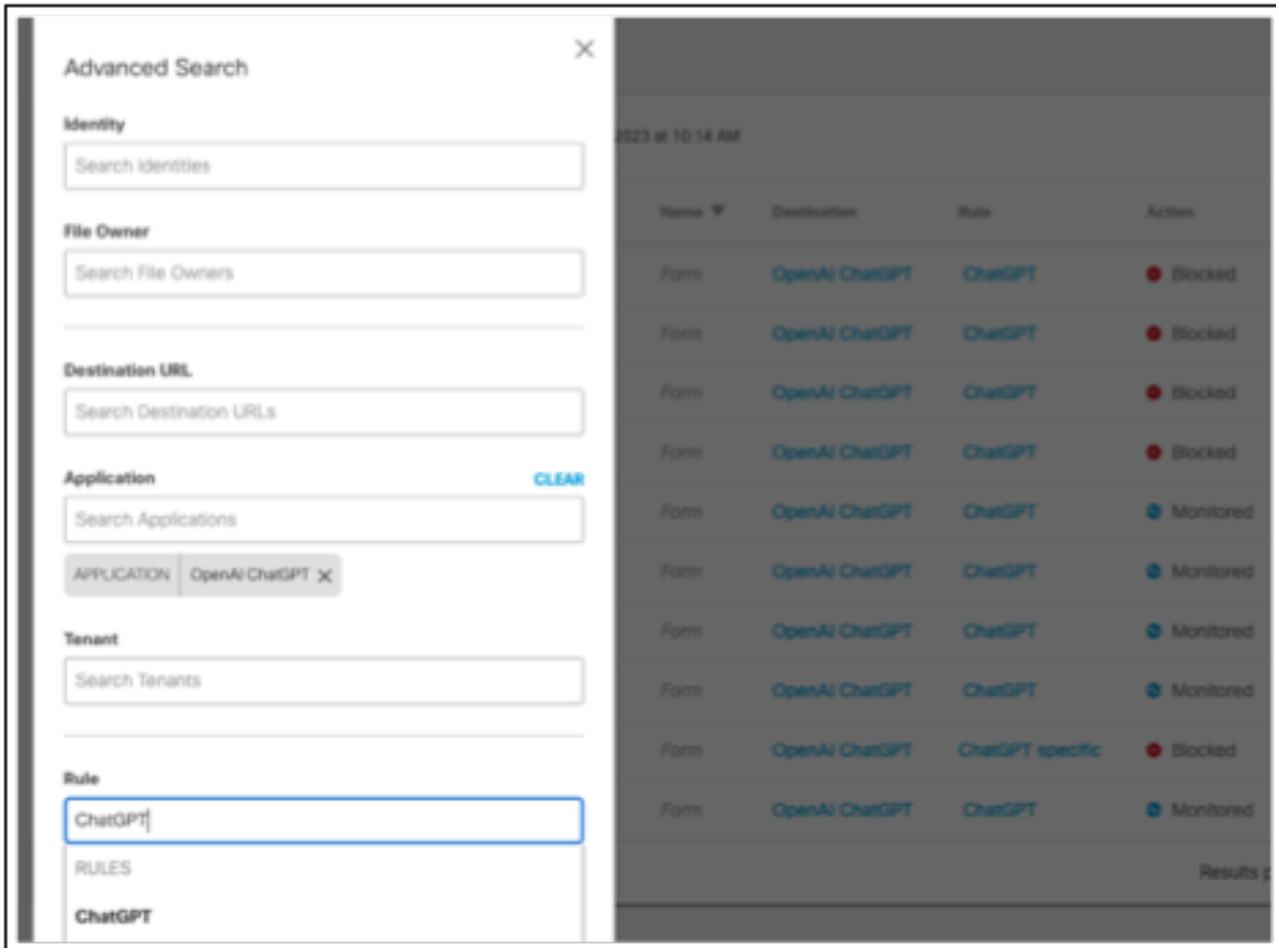
16221291406100

2. Controle granular sobre o acesso ao ChatGPT:
   Agora, os clientes podem bloquear o acesso ao ChatGPT para todos ou permitir o acesso apenas a usuários ou grupos de usuários específicos.
   Esse controle granular ajuda a gerenciar o uso do ChatGPT de acordo com os requisitos de segurança e conformidade. O bloqueio é possível por meio de políticas de DNS e da Web selecionando openAI ChatGPT em Configurações do aplicativo.



16221268217748

3. Avaliando o risco de uso de ChatGPT com DLP:
   O DLP em tempo real agora permite que os clientes monitorem o tipo de informações confidenciais que estão sendo enviadas e compartilhadas com o ChatGPT. Isso ajuda a avaliar o risco associado ao uso do ChatGPT e a tomar as medidas apropriadas para reduzir possíveis vazamentos ou violações de dados.
   Para ativar o monitoramento DLP para ChatGPT, os clientes podem utilizar regras em tempo real com o destino definido como Todos os destinos ou escolher openAI ChatGPT especificamente na lista de aplicativos disponíveis.



16221283948052

4. Permitindo o uso seguro de ChatGPT com DLP:
   Ao usar nossa solução DLP, os clientes agora podem bloquear solicitações ao ChatGPT que contêm informações confidenciais. Isso garante que os funcionários possam continuar a usar o ChatGPT com segurança, sem expor a organização a riscos em potencial.
   Para ativar o bloqueio de DLP para ChatGPT, os clientes podem utilizar regras em tempo real com o destino definido como Todos os destinos ou escolher openAI ChatGPT especificamente na lista de aplicativos disponíveis.

16221311959572

5. Evitar vazamento de código-fonte para ChatGPT com DLP:
   Com um novo identificador de dados de código fonte, os clientes podem usar o DLP para acompanhar e parar o compartilhamento de código fonte com o ChatGPT, protegendo sua valiosa propriedade intelectual (IP).

6. NOVA categoria de aplicação de IA geradora:
   Uma nova categoria de aplicação de IA gerativa foi introduzida para lidar com a descoberta e prevenção de uso para uma gama mais ampla de ferramentas.

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.