Konfigurieren der DLP- und CASB-Unterstützung für generative KI und ChatGPT

Inhalt

Einleitung

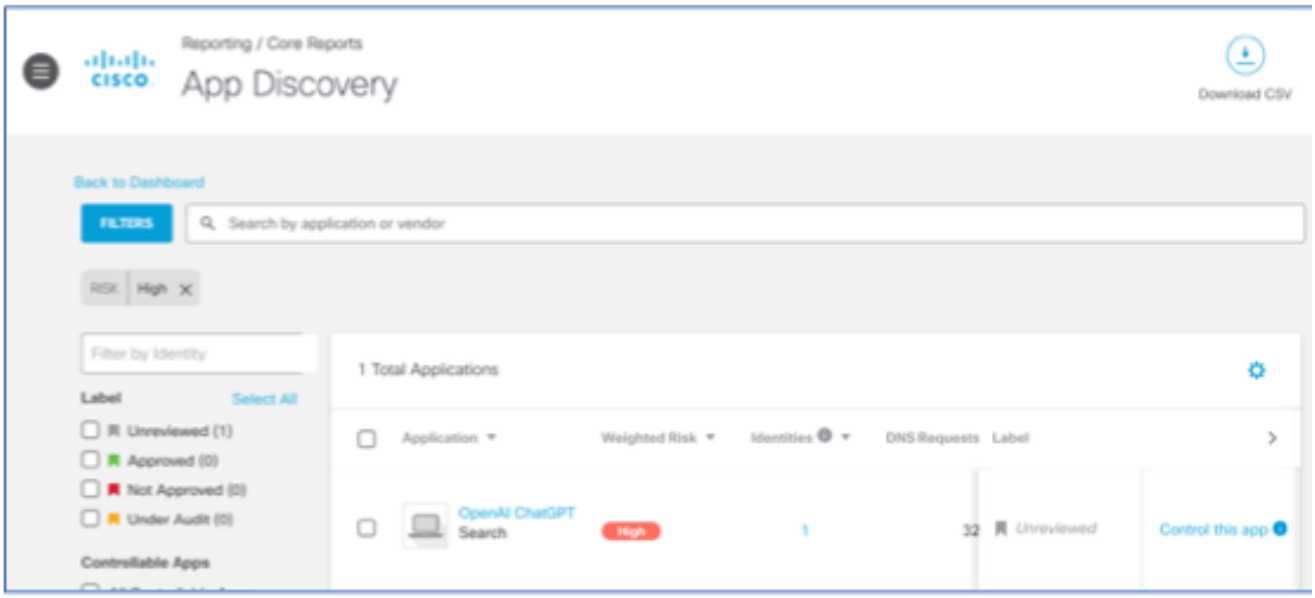
In diesem Dokument wird die Unterstützung von Cloud Access Security Broker (CASB) und Data Loss Prevention (DLP) für Generative AI und ChatGPT beschrieben.

Überblick

Wir haben neue Cloud Access Security Broker (CASB)- und Data Loss Prevention (DLP)-Erweiterungen für unsere Umbrella Produktsuite veröffentlicht, die Kunden dabei unterstützen sollen, die ChatGPT-Nutzung in ihren Unternehmen effektiver zu verwalten.
Mit diesen Erweiterungen können unsere Kunden sicherstellen, dass ihre Mitarbeiter ChatGPT verantwortungsbewusst und sicher nutzen und gleichzeitig vertrauliche Informationen vor potenziellen Risiken schützen.

Die wichtigsten Funktionen:

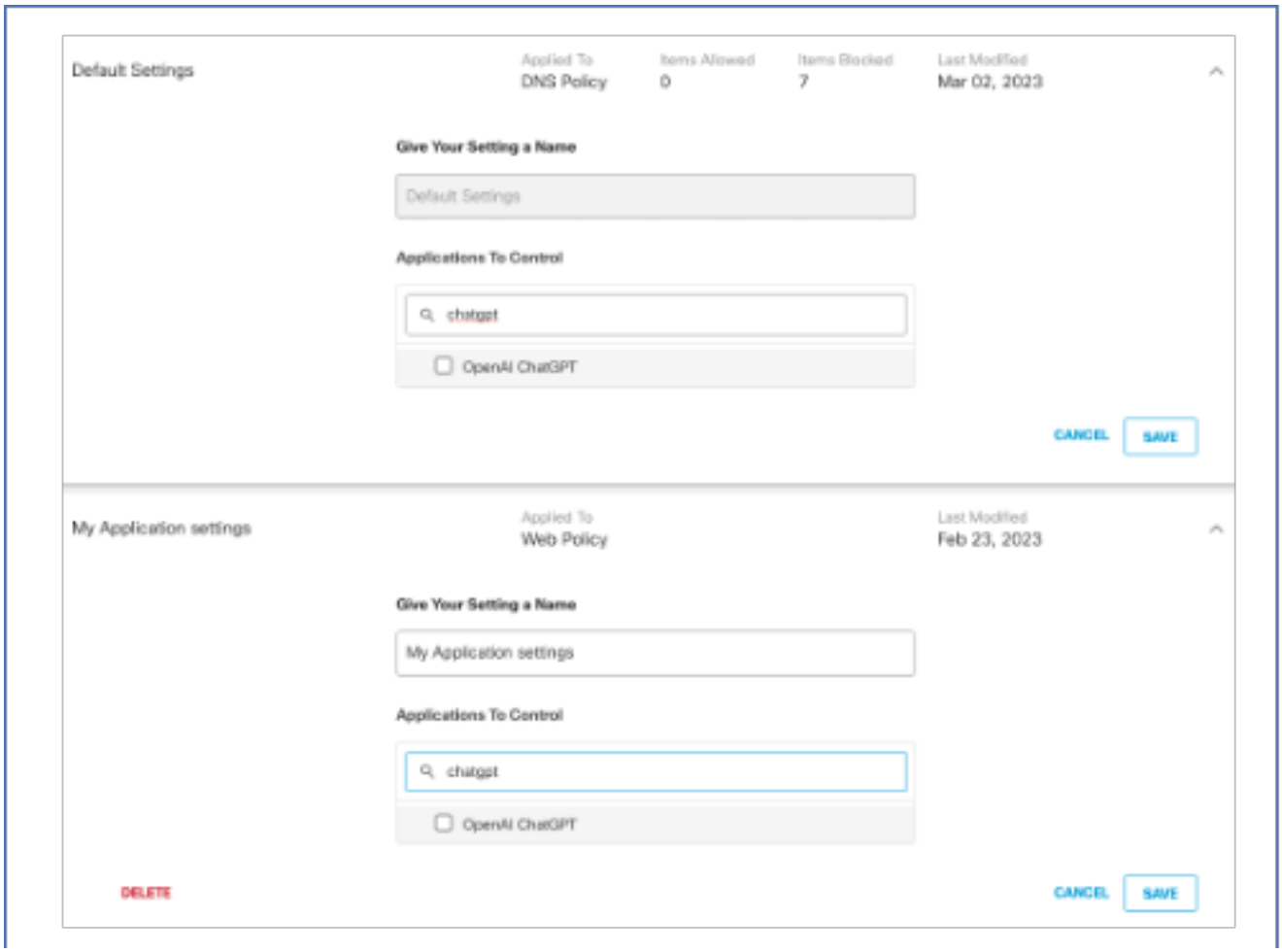
1. ChatGPT-Nutzung in der Organisation wird erkannt:
   Mithilfe des App Discovery-Berichts (Reports -> Core Reports) können Kunden die ChatGPT-Nutzung im gesamten Unternehmen identifizieren und überwachen.
   So erhalten sie wertvolle Einblicke in die Nutzung des Tools durch die Mitarbeiter, die es ihnen ermöglichen, seine Nutzung zu optimieren und die Einhaltung ihrer internen Richtlinien sicherzustellen.



16221272854164

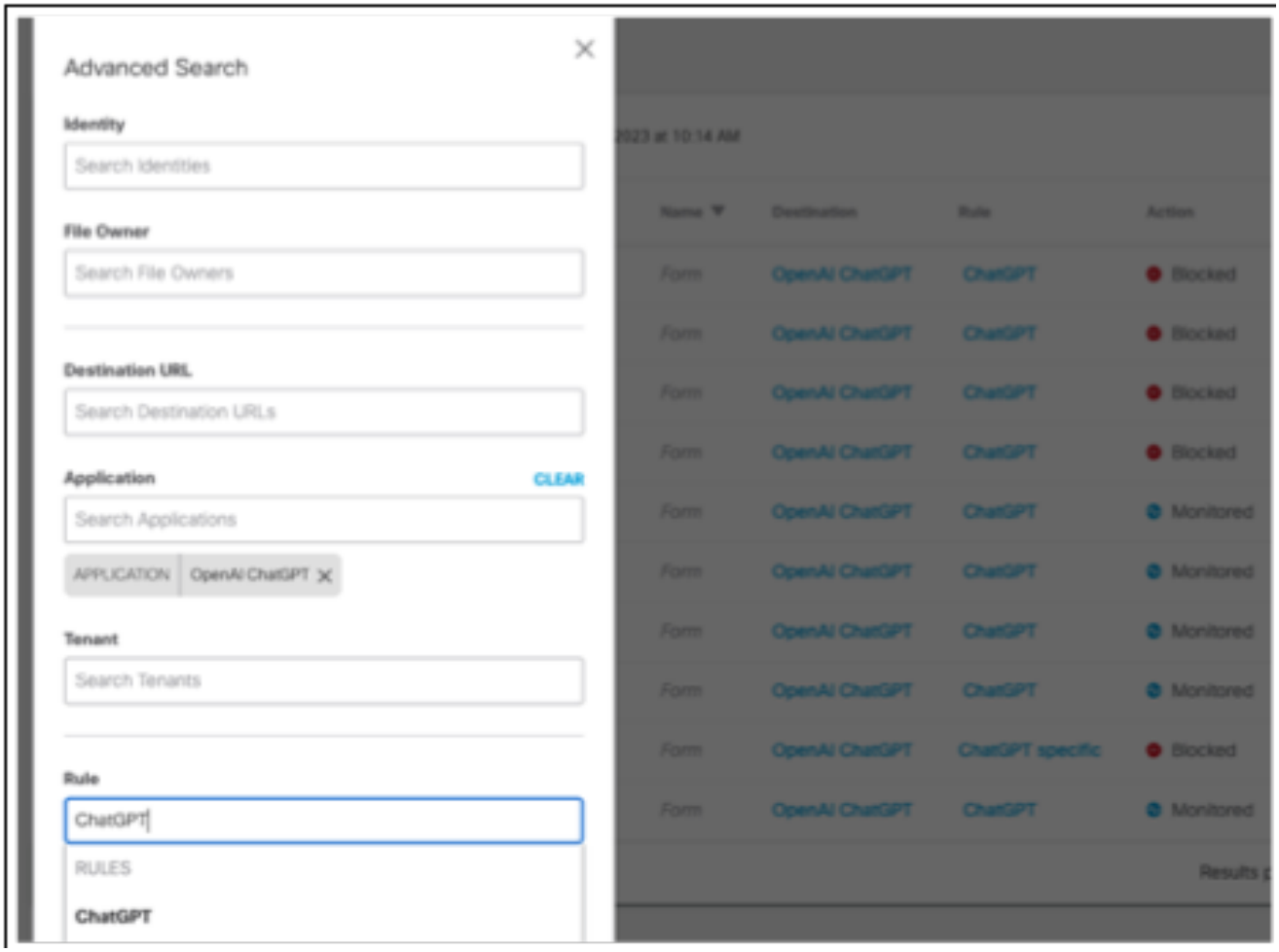
16221291406100

2. Präzise Kontrolle des ChatGPT-Zugriffs:
   Kunden können jetzt den Zugriff auf ChatGPT für alle Benutzer blockieren oder nur bestimmten Benutzern oder Benutzergruppen den Zugriff gestatten.
   Diese detaillierte Kontrolle hilft, die Nutzung von ChatGPT in Übereinstimmung mit den Sicherheits- und Compliance-Anforderungen zu verwalten. Die Sperrung ist sowohl über DNS- als auch über Webrichtlinien möglich, indem Sie in den Anwendungseinstellungen die Option openAI ChatGPT auswählen.



16221268217748

3. Bewertung des ChatGPT-Nutzungsrisikos mit DLP:
   Mithilfe von Echtzeit-SvD können Kunden jetzt den Typ der vertraulichen Informationen überwachen, die gesendet und für ChatGPT freigegeben werden. Dies hilft, die mit der ChatGPT-Nutzung verbundenen Risiken zu bewerten und geeignete Maßnahmen zu ergreifen, um potenzielle Datenlecks oder Sicherheitsverletzungen zu minimieren..
   Um die DLP-Überwachung für ChatGPT zu aktivieren, können Kunden entweder Echtzeitregeln verwenden, deren Ziel auf Alle Ziele festgelegt ist, oder openAI ChatGPT speziell aus der Liste der verfügbaren Anwendungen auswählen.



16221283948052

4. Sichere Verwendung von ChatGPT mit DLP:
   Mit unserer DLP-Lösung können Kunden jetzt Aufforderungen an ChatGPT blockieren, die vertrauliche Informationen enthalten. So wird sichergestellt, dass die Mitarbeiter ChatGPT weiterhin sicher und sicher nutzen können, ohne das Unternehmen potenziellen Risiken auszusetzen.
   Um die DLP-Blockierung für ChatGPT zu aktivieren, können Kunden entweder Echtzeitregeln verwenden, deren Ziel auf Alle Ziele festgelegt ist, oder openAI ChatGPT speziell aus der Liste der verfügbaren Anwendungen auswählen.

16221311959572

5. Verhindern von Quellcodeverlust in ChatGPT mit SvD:
   Mit einer neuen Quellcode-Daten-ID können Kunden DLP nutzen, um die gemeinsame Nutzung von Quellcode mit ChatGPT im Auge zu behalten und zu stoppen und so ihr wertvolles geistiges Eigentum (IP) zu schützen.

6. NEUE Anwendungskategorie für generative KI:
   Eine neue generative KI-Anwendungskategorie wurde eingeführt, um die Erkennung und Verhinderung der Nutzung für eine breitere Palette von Tools zu ermöglichen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.