Configurazione del supporto DLP e CASB per API generativa e ChatGPT

Sommario

Introduzione

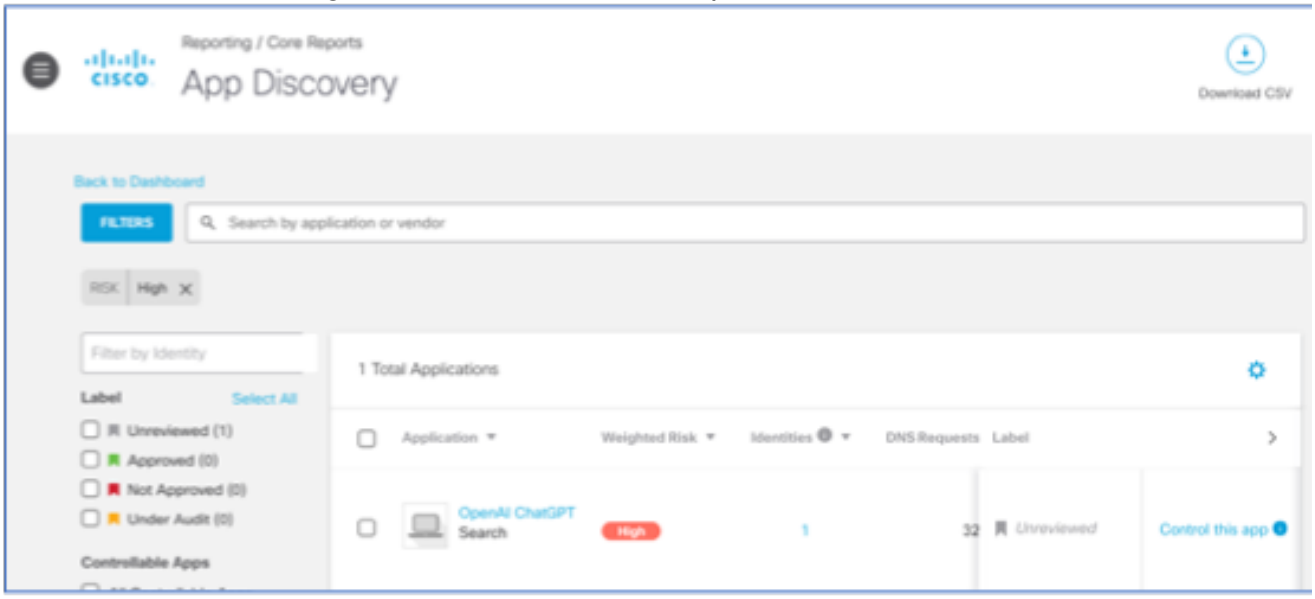
Questo documento descrive il supporto di Cloud Access Security Broker (CASB) e Data Loss Prevention (DLP) per Generative AI e ChatGPT.

Panoramica

Abbiamo rilasciato nuovi miglioramenti Cloud Access Security Broker (CASB) e Data Loss Prevention (DLP) per la nostra suite di prodotti Umbrella, progettati per aiutare i clienti a gestire l'utilizzo di ChatGPT all'interno delle loro organizzazioni in modo più efficace.
Questi miglioramenti consentono ai nostri clienti di garantire che i loro dipendenti utilizzino ChatGPT in modo responsabile e sicuro, proteggendo al contempo le informazioni riservate da potenziali rischi.

Ecco le caratteristiche principali:

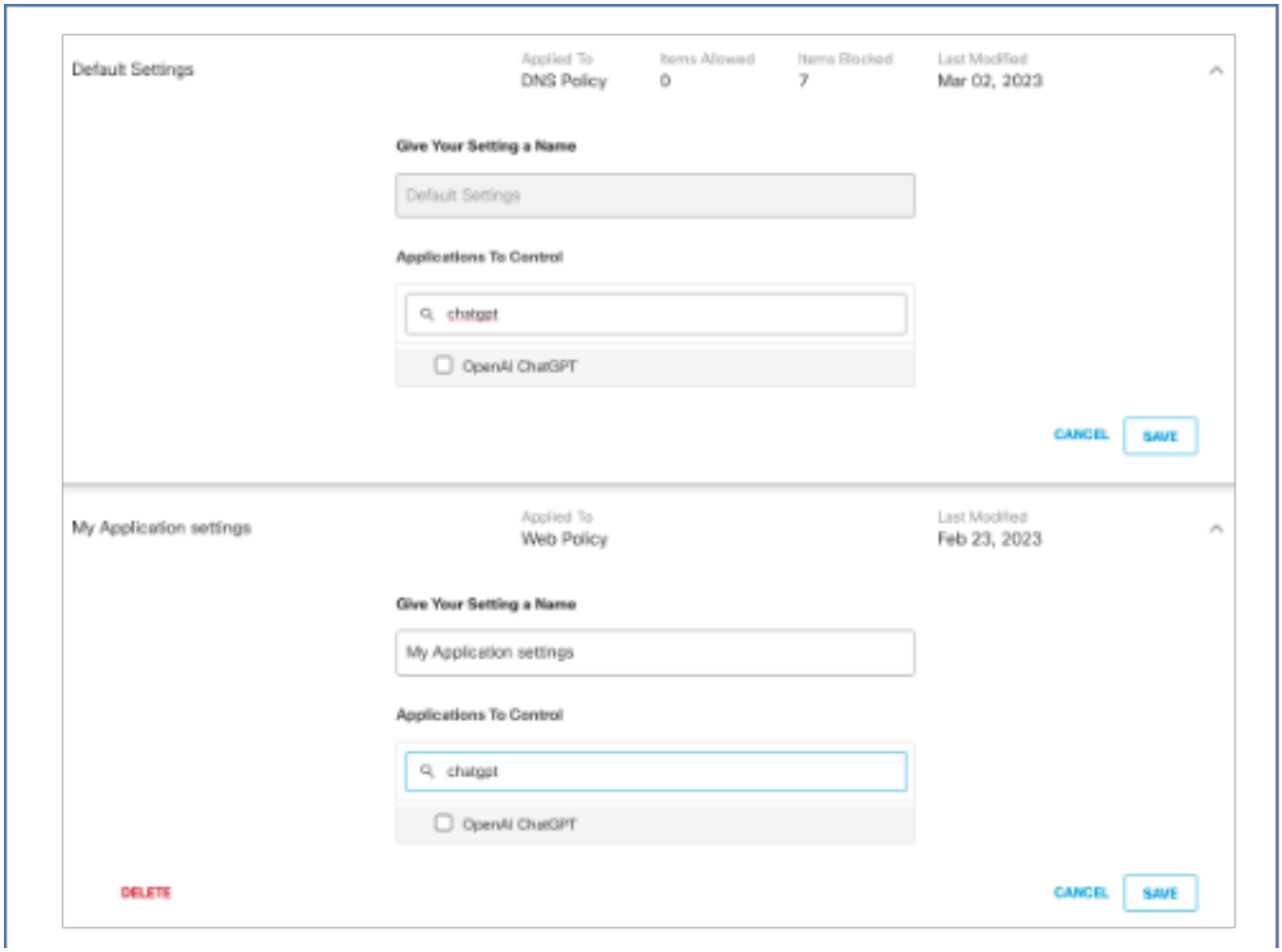
1. Individuazione dell'utilizzo di ChatGPT nell'organizzazione:
   Utilizzando il report di individuazione applicazioni (Report -> Report principali), i clienti possono identificare e monitorare l'utilizzo di ChatGPT nell'organizzazione.
   In questo modo i dipendenti possono ottenere informazioni utili sull'utilizzo dello strumento, ottimizzarne l'utilizzo e garantire la conformità alle politiche interne.



16221272854164

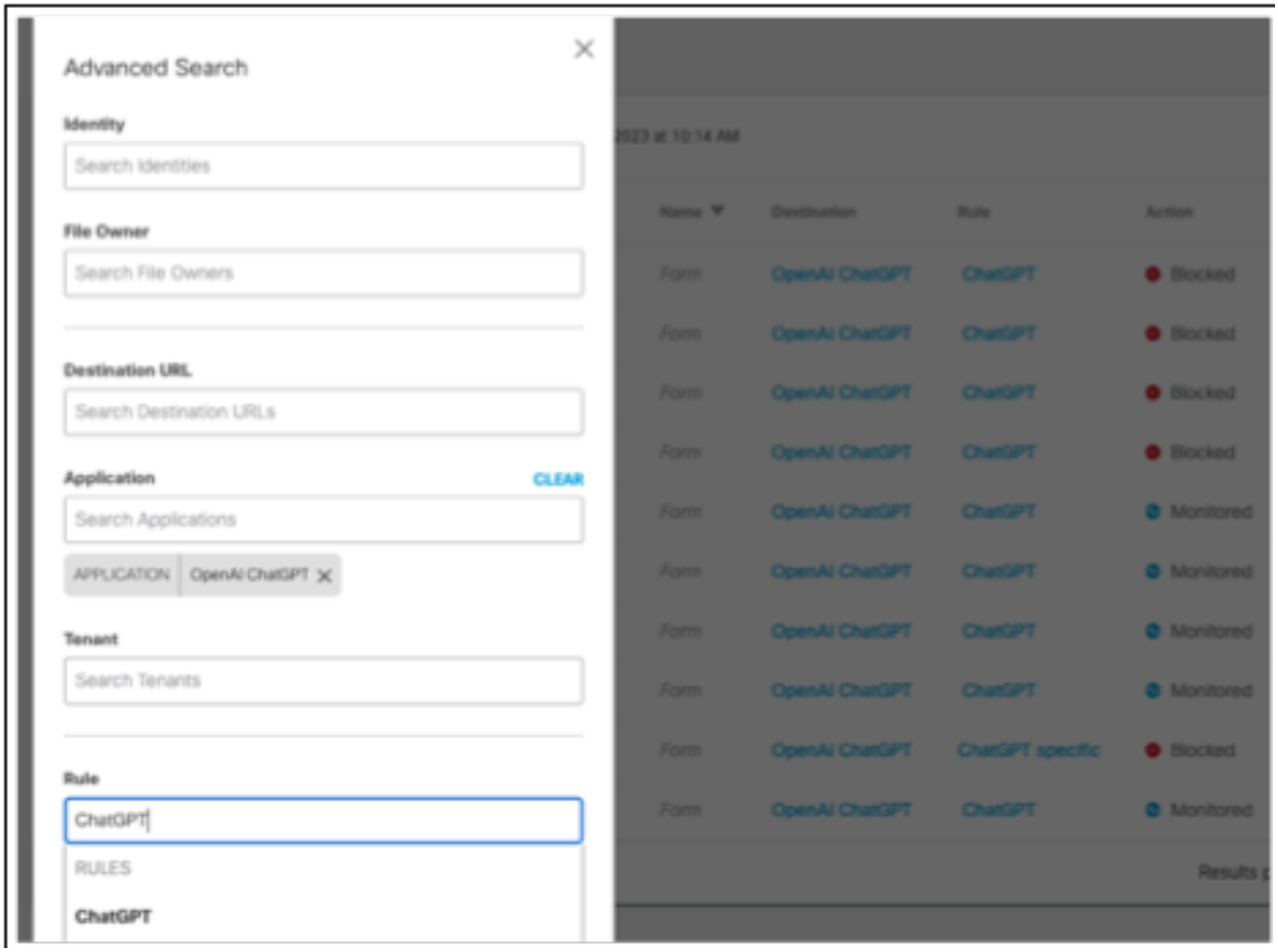
16221291406100

2. Controllo granulare sull'accesso ChatGPT:
   I clienti possono ora bloccare l'accesso a ChatGPT per tutti o consentire l'accesso solo a utenti o gruppi di utenti specifici.
   Questo controllo granulare consente di gestire l'utilizzo di ChatGPT in linea con i requisiti di sicurezza e conformità. Il blocco è possibile tramite i criteri DNS e Web selezionando openAI ChatGPT in Impostazioni applicazione.



16221268217748

3. Valutazione del rischio di utilizzo di ChatGPT con DLP:
   Real Time DLP consente ai clienti di monitorare il tipo di informazioni riservate inviate e condivise con ChatGPT. In questo modo è possibile valutare i rischi associati all'utilizzo di ChatGPT e adottare misure appropriate per ridurre potenziali perdite di dati o violazioni.
   Per abilitare il monitoraggio DLP per ChatGPT, i clienti possono utilizzare le regole in tempo reale con la destinazione impostata su Tutte le destinazioni o scegliere openAI ChatGPT specificamente dall'elenco delle applicazioni disponibili.



16221283948052

4. Consentire l'utilizzo sicuro di ChatGPT con DLP:
   Utilizzando la soluzione DLP, i clienti possono ora bloccare le richieste di ChatGPT che contengono informazioni riservate. Ciò garantisce che i dipendenti possano continuare a utilizzare ChatGPT in modo sicuro, senza esporre l'organizzazione a potenziali rischi.
   Per abilitare il blocco DLP per ChatGPT, i clienti possono utilizzare le regole in tempo reale con la destinazione impostata su Tutte le destinazioni o scegliere openAI ChatGPT specificamente dall'elenco delle applicazioni disponibili.

16221311959572

5. Prevenzione di perdite di codice sorgente in ChatGPT con DLP:
   Grazie a un nuovo identificatore dei dati del codice sorgente, i clienti possono utilizzare il DLP per controllare e interrompere la condivisione del codice sorgente con ChatGPT, salvaguardando la loro preziosa proprietà intellettuale (IP).

6. NUOVA categoria di applicazioni API generative:
   È stata introdotta una nuova categoria di applicazioni di IA generativa per affrontare l'individuazione e la prevenzione dell'utilizzo per una più ampia gamma di strumenti.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).