Scopri come la forza lavoro può utilizzare la shadow AI e lo shadow IT

Estendi la visibilità sugli strumenti IA e SaaS non autorizzati con l'ispezione del traffico di Cloudflare

Smascherare l'invisibile

Lo shadow IT non è un problema nuovo, ma la rapida adozione di strumenti di intelligenza artificiale non approvati sta provocando una crisi moderna:

- Il **20%** delle organizzazioni ha subito una violazione a causa di incidenti di sicurezza con la shadow AI nel 2025[1]
- L'**85%** dei responsabili IT afferma che i dipendenti stanno adottando strumenti di intelligenza artificiale prima che l'IT possa valutarli[2]

Cloudflare ripristina la visibilità per consentire alle organizzazioni di gestire questa superficie d'attacco in espansione:

- **Rivedere lo stato delle app:** classifica le app IA e SaaS come approvate, non approvate o ancora in fase di revisione
- **Applicare politiche in base allo stato dell'app:** consenti, blocca, isola, applica rilevamenti DLP alle interazioni, limita i caricamenti di file e altro ancora
- **Analizzare l'utilizzo delle app:** monitora le tendenze aggregate e conduci indagini dettagliate
- **Valutare il rischio dell'app:** valuta l'affidabilità tramite i punteggi di affidabilità dell'applicazione

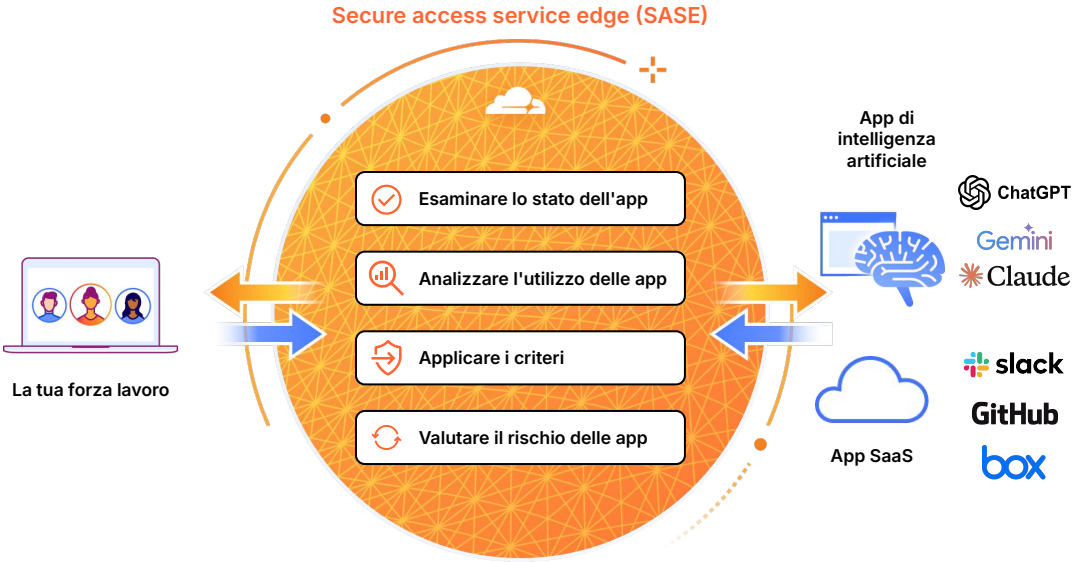
Rischi unici della shadow AI

La shadow AI è una cosa diversa dallo shadow IT tradizionale. Mentre le app SaaS archiviano o condividono principalmente file, gli strumenti di intelligenza artificiale si trasformano e imparano da qualsiasi input dei dipendenti.

Ciò significa che IP sensibili, dati dei clienti o codice sorgente possono essere assorbiti in modo irreversibile per l'addestramento del modello senza possibilità di rimozione.

Come funziona

La piattaforma SASE di Cloudflare si integra tra la tua forza lavoro e le tue risorse per unificare visibilità e controlli.



Inoltre, integra il CASB di Cloudflare tramite API per eseguire la scansione di configurazioni errate, attività degli utenti e dati sensibili.
Gestisci lo stato di sicurezza tra le app di intelligenza artificiale (ChatGPT, Claude, Google Gemini) e altre app SaaS.
Utilizza CASB con il tuo provider di identità per vedere quando gli utenti si autenticano su app di terze parti non autorizzate.

Dashboard di esempio

Filtra questa panoramica di alto livello sull'utilizzo delle app in base a:

- Applicazione e tipo di app
- Stato di approvazione
- Protezione con ZTNA
- Numero di utenti

Per maggiori dettagli, clicca sul nome di un'app di intelligenza artificiale per vedere gli utenti o i gruppi specifici che vi accedono, la frequenza di utilizzo, la posizione e la quantità di dati trasferiti.

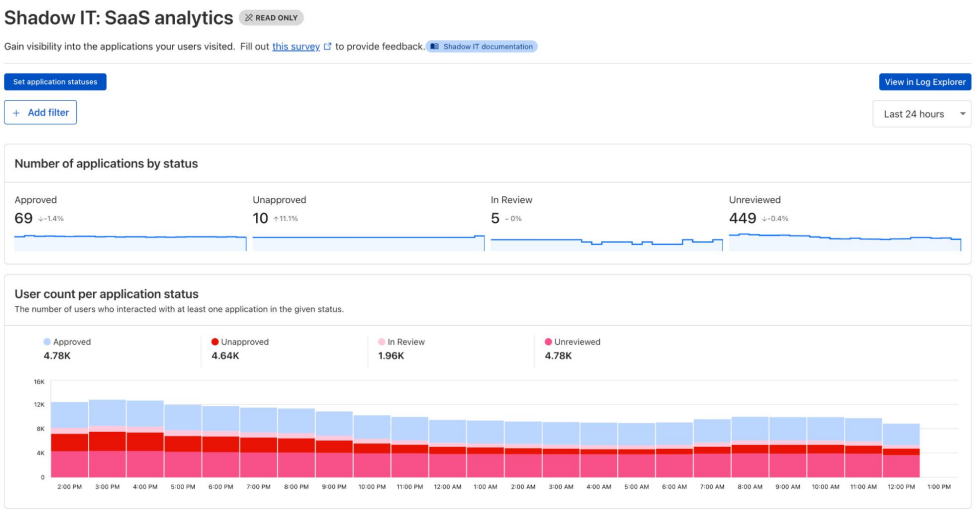


Figura 1: dashboard di analisi dello shadow IT

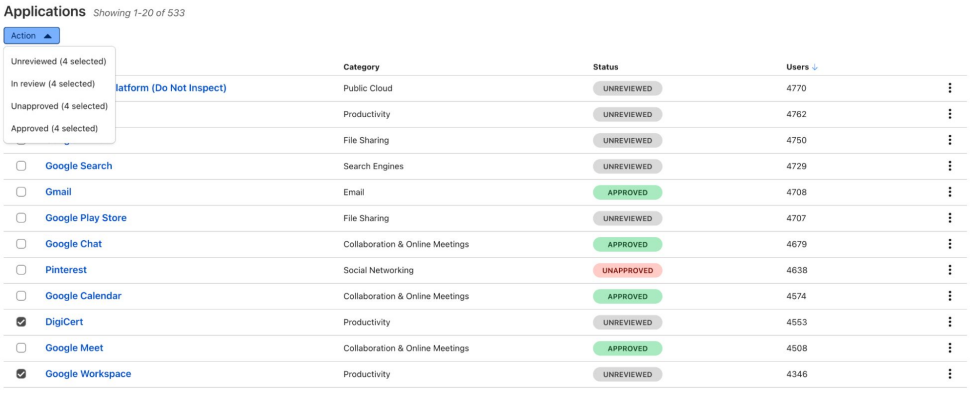


Figura 2: contrassegno degli stati delle applicazioni

Organizza le app e imposta i criteri di accesso in base allo stato di approvazione:

- Approvato (autorizzato)
- Non approvato (non autorizzato)
- In fase di revisione
- Non revisionato

Hai bisogno di altre indicazioni tecniche? Scopri come creare criteri con questo percorso di apprendimento.

Vuoi approfondire come proteggere l'adozione dell'intelligenza artificiale?

Esplora altri casi d'uso | **Richiedi un workshop**

1. 2025 IBM, report Cost of a Data Breach report: Fonte
2. Ricerca Manage Engine 2025: Fonte

