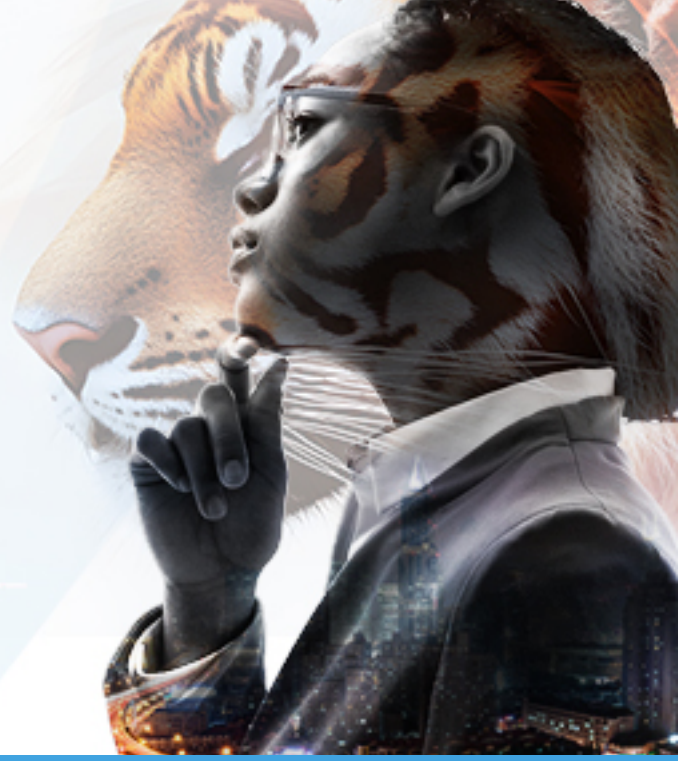
COPILOT
CON SYMANTEC DLP



PROTEGGI I TUOI DATI PRIMA DI ABILITARE COPILOT CON SYMANTEC DLP

Come molti strumenti di IA generativa, **Microsoft Copilot** apre le porte alla produttività, ma comporta anche dei rischi. Integrato in tutta la piattaforma di Microsoft 365, può potenzialmente accedere a qualsiasi documento, presentazione, e-mail, foglio di calcolo e altro ancora.

Questo include i tuoi dati più preziosi e sensibili. **Per utilizzare Copilot in modo sicuro e produttivo**, è necessario definire i confini fin dall'inizio (con la corretta governance dei dati).

SFIDE E RISCHI

Le aree chiave da risolvere prima di implementare Copilot!

COME REALIZZERAI IL TUO SISTEMA DLP?

Se stai già utilizzando Symantec DLP, ci sono buone notizie: è facile estenderlo per fornire la governance dei dati per Copilot. Se devi creare un sistema da zero, scegli una soluzione leader di mercato che copra tutti gli aspetti.

Symantec DLP è rinomato per la sua accuratezza nel rilevamento, la piena integrazione con MSFT e la distribuzione su larga scala; inoltre, può aiutarti a trovare, classificare ed etichettare rapidamente i dati sensibili.

1. IDENTIFICAZIONE DEI DATI SENSIBILI

Per proteggere i tuoi dati riservati, devi prima trovarli, ispezionarli per verificare la presenza di contenuti sensibili ed etichettarli correttamente. La sfida è che hai bisogno di un approccio coerente e accurato. Un approccio che funziona su dati che non sono stati toccati per un po', riflette le tue ultime policy di sicurezza dei dati ed è ripetibile (in quale altro modo potresti proteggere i nuovi dati generati).

Symantec DLP fa tutto questo e si integra con Microsoft Purview per garantire che Copilot sappia con cosa può interagire e cosa non fare.

RISCHIO	**Un Copilot désorienté pourrait ne pas identifier vos documents confidentiels, augmentant ainsi le risque de fuite de données.**

2. ETICHETTATURA DI NUOVI CONTENUTI

Il contenuto generato da Copilot **non eredita automaticamente le etichette di sicurezza dei suoi file di origine.**

Ciò lascia i dipendenti liberi di stabilire se i nuovi contenuti debbano essere classificati come riservati.

RISCHIO	**I dipendenti possono vedere e condividere informazioni sensibili da documenti etichettati in modo errato.**

3. AUTORIZZAZIONI ECCESSIVE

Copilot adotta gli stessi diritti di accesso dei suoi utenti, ma spesso i dipendenti hanno più autorizzazioni di quante dovrebbero. Ciò consente a Copilot di accedere a contenuti sensibili e di condividerli con utenti non autorizzati.

RISCHIO	**L'"eccesso di autorizzazioni" aumenta il rischio di accesso non autorizzato ai dati e di esposizione.**

4. INTEGRAZIONE CON MICROSOFT 365

Tutto quanto sopra è reso più difficile a causa della **profonda integrazione di Copilot con la famiglia Microsoft 365.** Ciò aggiunge complessità alla governance dei dati, rendendo più difficile mantenere la visibilità e applicare l'accesso con privilegi minimi.

RISCHIO	**Maggiore è la portata e la complessità, maggiore sarà il rischio di esposizione dei dati.**

SYMANTEC DLP – IL MODO MIGLIORE PER ABILITARE COPILOT

Symantec DLP offre vantaggi unici alle organizzazioni che implementano Copilot. L'integrazione perfetta con Microsoft 365 semplifica l'applicazione di una governance coerente dei dati in tutto l'ecosistema, proteggendo i dati ovunque si trovino.

LA SOLUZIONE AUTOMATIZZATA

Controlla il contenuto per rilevare dati sensibili, inclusi file non etichettati o classificati in modo errato

Corregge i dati classificati in modo errato, applicando le etichette giuste in base alle policy di DLP

Ispeziona, classifica ed etichetta tutti i nuovi contenuti generati da Copilot

Classifica i file e utilizza la tecnologia di Microsoft per applicare l'etichetta di sensibilità, garantendo che Copilot riconosca i dati sensibili

Applica le policy di DLP esistenti in Microsoft 365 per garantire la coerenza (anche per l'archiviazione e i contenuti ancora da generare)

PROTEZIONE DEI DATI SEMPLICE E UNIFICATA

L'utilizzo sicuro di Copilot richiede una solida governance dei dati. Grazie a Symantec DLP, tutto questo non deve essere per forza complesso.

Per scoprire come funziona in pratica, contattaci oggi stesso.