

Le Skill AI: il nuovo rischio invisibile in azienda

Pochi click, un permesso da confermare, e l'agente AI sa fare qualcosa in più. Ma raramente qualcuno controlla davvero cosa c'è dentro quel pacchetto di codice.

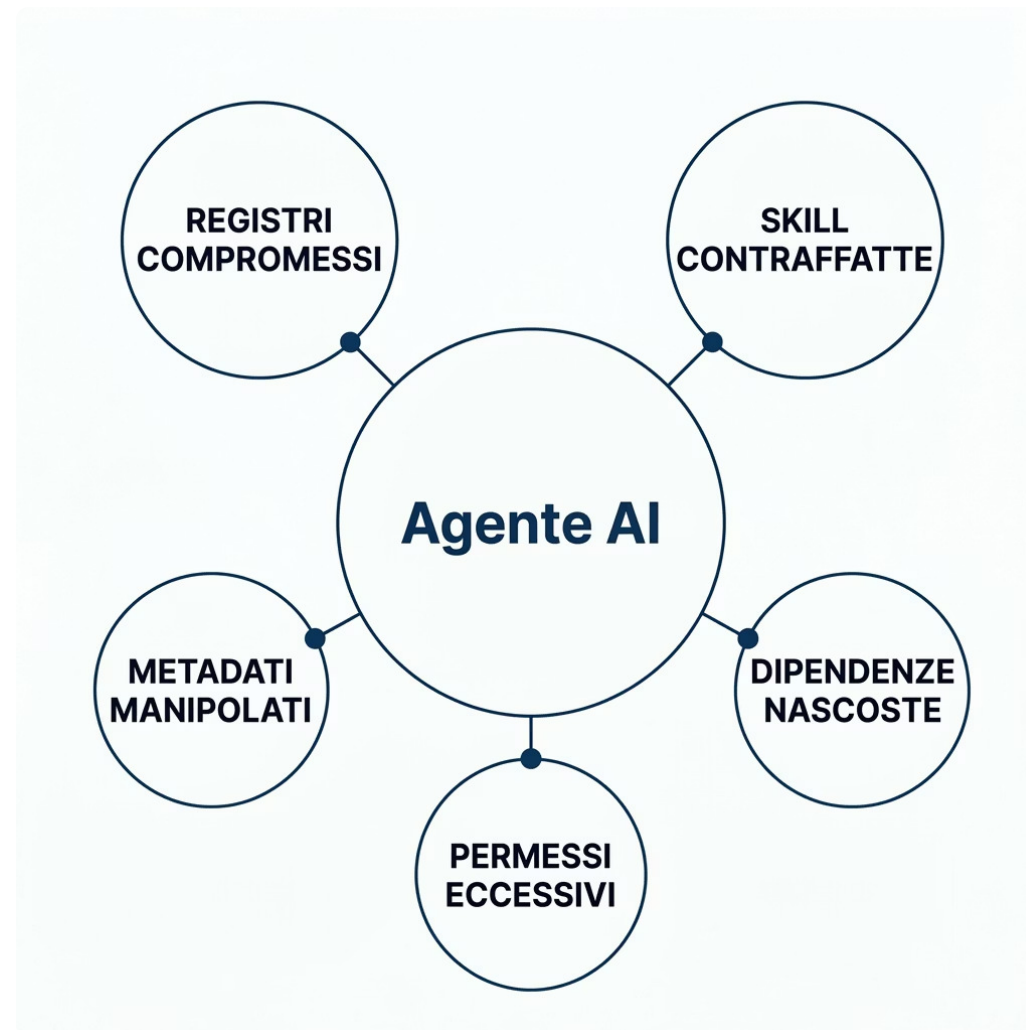
SICUREZZA AI

SUPPLY CHAIN SOFTWARE

Un ecosistema in rapida crescita

Sempre più aziende collegano ai propri strumenti AI funzioni aggiuntive scaricabili da repository pubblici o marketplace di terze parti — chiamate **skill, plugin o estensioni**.

Questi ecosistemi stanno diventando una nuova supply chain software, con gli stessi rischi delle librerie open source e **nessuno dei controlli** maturati da store consolidati come Apple o Google.



I rischi della nuova supply chain AI

Registri compromessi

Repository pubblici falsificati o alterati alla fonte.

Skill contraffatte

Imitano quelle legittime per ingannare l'installatore.

Dipendenze nascoste

Pacchetti collegati tra loro in modo non trasparente.

Metadati manipolati

Fanno apparire una skill più affidabile di quanto sia.

Perché riguarda anche le PMI

Un centralino AI, un assistente ordini o un agente clienti funziona collegando più moduli tra loro. Ogni modulo esterno è, di fatto, **un fornitore in più** con accesso ai dati aziendali.

Lettura conversazioni

Una skill compromessa può accedere ai dialoghi con i clienti.

Accesso al gestionale

Può leggere o modificare dati nei sistemi collegati.

Azioni non autorizzate

Si maschera da funzione legittima per agire indisturbata.

Le domande da farsi prima di installare



Rispondere "no" anche a una sola di queste domande è un segnale d'allerta da non ignorare.

Un fornitore critico, non un dettaglio tecnico

Non serve rinunciare agli agenti AI per essere al sicuro. Serve trattarli come quello che sono già diventati: un altro fornitore critico dentro l'azienda.

Le stesse domande di sicurezza che ci si farebbe con chiunque gestisca dati sensibili per conto tuo vanno applicate anche alle skill AI.

Punti chiave da portare con sé

01

Tratta ogni skill come un fornitore

Accesso ai dati = responsabilità da valutare.

02

Verifica provenienza e permessi

Autore verificabile, permessi coerenti con la funzione dichiarata.

03

Testa in ambiente isolato

Prima di collegare ai sistemi reali, isola e osserva il comportamento.

04

Chiedi garanzie al fornitore AI

La verifica preventiva del codice deve essere parte del servizio.



La sicurezza degli agenti AI inizia dalle stesse domande che fai a qualsiasi altro fornitore.