

# Il Messaggero

Economia

**ECONOMIA - NAZIONALE; Engineering, Bisio: con gli agenti cambia la natura degli attacchi**

Giacomo Andreoli

334 words

16 October 2026

Il Messaggero

MSGO

Italian

© 2026. Il Messaggero

Engineering lancia EngSure, una piattaforma che utilizza l'intelligenza artificiale per individuare le minacce informatiche e proteggere dati, modelli e applicazioni basati sull'AI. La soluzione, annunciata al Digital Innovation Forum 2026, punta a rendere più sicuro l'impiego degli agenti intelligenti, sistemi capaci di svolgere attività, accedere a informazioni e utilizzare strumenti con un certo grado di autonomia.

«La diffusione dell'AI agentica sta cambiando profondamente anche la natura degli attacchi informatici. Non basta più difendere il perimetro delle organizzazioni: occorre proteggere e sorvegliare gli agenti, verificare i dati su cui apprendono e controllare il modo in cui prendono decisioni», ha spiegato Aldo Bisio, amministratore delegato di Engineering.

EngSure si articola in quattro moduli: Shield controlla i sistemi in funzione e individua anomalie e attacchi; Probe simula tentativi di intrusione per scoprire punti deboli; Certis raccoglie le prove necessarie per verifiche e controlli; Provenance esamina origine, qualità e affidabilità di dati e modelli. La piattaforma può anche rilevare quando un agente tenta di accedere a informazioni o compiere operazioni non autorizzate, bloccandolo o chiedendo l'intervento di una persona. I controlli possono essere adattati al livello di rischio delle attività svolte.

«EngSure mette a disposizione di imprese e Pubbliche Amministrazioni strumenti per presidiare l'intera filiera dell'AI, dal dato fino al controllo del comportamento degli agenti», ha aggiunto Bisio. La soluzione si inserisce nella strategia Is-Ia di Engineering, dedicata alla gestione e al controllo dell'intelligenza artificiale, e permette di integrare verifiche di sicurezza nelle diverse fasi di utilizzo, dalla valutazione prima del rilascio alla sorveglianza durante il funzionamento.

Il sistema è progettato per operare con modelli e infrastrutture differenti, adattando i controlli alle caratteristiche delle applicazioni e alle esigenze delle organizzazioni. In questo modo, le imprese possono individuare eventuali vulnerabilità prima che vengano sfruttate e verificare che gli agenti rispettino le autorizzazioni ricevute, con livelli di supervisione umana definiti in base alla delicatezza delle operazioni.

Document MSGO000020261016emag0006f