

VINCENZO CALABRÒ

Shadow AI

L'intelligenza artificiale non autorizzata
nelle organizzazioni

COS'È LA SHADOW AI?

Definizione

La Shadow AI si riferisce all'uso di strumenti, modelli o sistemi di intelligenza artificiale all'interno di un'organizzazione senza l'approvazione, la supervisione o la conoscenza del dipartimento IT o della direzione.



Chatbot AI

ChatGPT, Claude, Gemini usati per lavoro senza autorizzazione



Generatori di Immagini

Midjourney, DALL-E per campagne marketing non approvate



AI per il Codice

GitHub Copilot, Cursor usati da sviluppatori senza policy

LA DIMENSIONE DEL FENOMENO

75%

dei dipendenti
usa AI non approvata

65%

delle aziende non ha
policy chiare sull'AI

3x

più rapido l'adozione
rispetto alla governance

48%

dati sensibili condivisi
con AI esterni



Trend di Adozione della Shadow AI (2021–2024)

L'uso di strumenti AI non autorizzati è cresciuto esponenzialmente con la diffusione di ChatGPT (2022) e dei modelli multimodali (2023–2024). Le stime indicano che oltre tre quarti dei knowledge worker utilizzano almeno uno strumento AI esterno non approvato dalla propria organizzazione.

PERCHÉ EMERGE LA SHADOW AI?



Pressione sulla Produttività

I dipendenti cercano strumenti che aumentino la loro efficienza senza aspettare processi di approvazione lenti.



Policy IT Troppo Restrittive

Regole rigide o poco chiare spingono i lavoratori a trovare soluzioni alternative in modo autonomo.



Rapida Evoluzione Tecnologica

I nuovi strumenti AI emergono più velocemente di quanto le organizzazioni possano valutarli e approvare.



Scarsa Formazione

I dipendenti non sanno quali strumenti sono approvati o comprendono i rischi degli strumenti non autorizzati.



Vantaggio Competitivo Percepito

I professionisti temono di restare indietro rispetto ai colleghi che usano AI più avanzate.



Frustrazione con gli Strumenti Ufficiali

I tool aziendali approvati sono spesso meno potenti o più difficili da usare rispetto alle alternative esterne.

I RISCHI PRINCIPALI

Violazione dei Dati

CRITICO

Dati sensibili, PII o segreti aziendali condivisi con LLM esterni e memorizzati da terze parti.

Non Conformità Normativa

ALTO

Violazione di GDPR, HIPAA, SOC 2 e altri standard per mancato controllo sul trattamento dei dati.

Rischi di Sicurezza

ALTO

Superfici di attacco ampliate, prompt injection, e perdita di controllo sulle credenziali di accesso.

Output Inaffidabili

MEDIO

Decisioni aziendali basate su allucinazioni AI non verificate o informazioni obsolete.

Impatto Potenziale

Multa GDPR

fino a €20M

Data breach costo medio

\$4.45M

Danno reputazionale

Incalcolabile

Perdita di IP

Permanente

Responsabilità legale

Dirigenti

COME RILEVARE LA SHADOW AI

01



Network Monitoring

Analisi del traffico di rete per identificare connessioni verso domini AI noti (openai.com, anthropic.com, etc.)

02



Shadow IT Discovery

Strumenti CASB e SaaS discovery per mappare tutte le applicazioni in uso non approvate

03



Audit & Survey

Questionari anonimi e interviste per comprendere i bisogni reali dei dipendenti

04



AI Governance Tools

Piattaforme dedicate (Lakera, Prompt Security) per monitorare l'uso di LLM nell'organizzazione

STRATEGIE DI RISPOSTA

✓ APPROCCIO CONSIGLIATO

- ✓ Creare una AI policy chiara e accessibile
- ✓ Approvare strumenti AI sicuri e certificati
- ✓ Formare i dipendenti sui rischi e best practice
- ✓ Istituire un AI Center of Excellence
- ✓ Promuovere canali ufficiali per proporre nuovi tool
- ✓ Implementare soluzioni enterprise (Azure OpenAI, Vertex AI)

✗ COSA EVITARE

- ✗ Bloccare tutto l'accesso all'AI (genera resistenza)
- ✗ Ignorare il fenomeno sperando che passi
- ✗ Policy vaghe o non comunicate efficacemente
- ✗ Mancanza di alternative ufficiali ai tool popolari
- ✗ Controlli punitivi senza educazione preventiva
- ✗ Trattare tutti gli strumenti AI allo stesso modo

Policy & Compliance

AI Acceptable Use Policy
Registro strumenti approvati
Valutazione rischi periodica
Allineamento a GDPR / EU AI Act

Sicurezza & Controllo

CASB per monitoraggio SaaS
DLP per prevenire data leakage
SSO e gestione accessi
Audit trail delle interazioni AI

Formazione & Cultura

Training obbligatorio sull'AI
Comunicazione policy chiara
Champion program per business unit
Canale feedback per nuovi tool

Abilitazione & Innovazione

Sandbox per sperimentazione sicura
Processo fast-track di approvazione
AI tool marketplace interno
Pilot program strutturati

CONCLUSIONI CHIAVE

La Shadow AI non è un problema da eliminare, è un'opportunità da governare.



I dipendenti usano la Shadow AI per essere più produttivi — questa è un'informazione preziosa.



Il problema non è l'AI, ma la mancanza di governance, policy e alternative ufficiali.



La risposta vincente è abilitare in modo sicuro, non bloccare in modo cieco.



Implementare un framework di governance proattivo prima che il problema diventi crisi.

VINCENZO CALABRÒ

Thanks!

