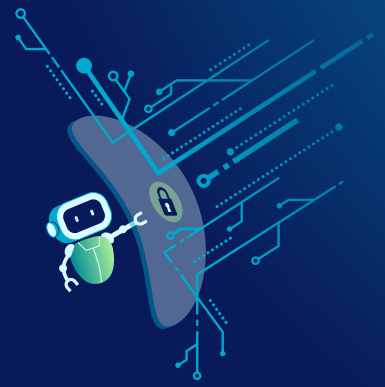
netskope

AI Security Checklist

Una guida pratica per CISO e team di Security su come proteggere l'utilizzo dell'AI

AI Security Checklist



Le aziende stanno adottando l'AI a un ritmo serrato, mettendo i team di sicurezza sotto pressione per garantire le fondamenta necessarie a un'implementazione sicura. Nella corsa ai benefici dell'AI, è vitale però che le organizzazioni non saltino passaggi fondamentali.

Questa checklist raccoglie le domande più importanti da porsi mentre si esamina il proprio ambiente, le policy e i controlli.
È pensata per aiutare i responsabili della sicurezza a valutare rapidamente lo stato attuale e capire cosa fare dopo, permettendo di trovare le lacune, stabilire le priorità delle azioni e capire con fiducia dove concentrare le attività.

Scoprire

Identificare tutti gli usi dell'AI in azienda

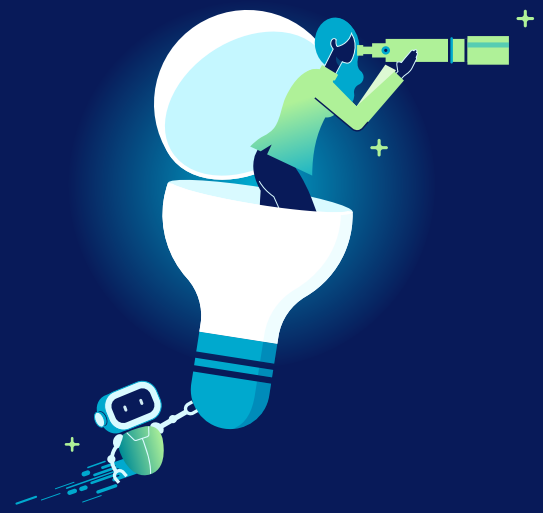
Di recente, abbiamo assistito a un'esplosione di strumenti di intelligenza artificiale nelle aziende, non tutti evidenti ai professionisti della sicurezza. LA Shadow AI rimane un problema: Il 47% degli utenti usa ancora app di AI personali al lavoro (Netskope, 2026 Cloud and Threat Report). Esiste anche la possibilità che l'attuale portafoglio di applicazioni SaaS aggiunga funzioni di intelligenza artificiale che aumentano il rischio per i dati. I team di sicurezza devono esaminare attentamente ogni strumento per valutare il suo impatto sull'AI.

Da valutare

Abbiamo visibilità su tutti gli strumenti di intelligenza artificiale gestiti e non gestiti?

Possiamo individuare le funzioni di intelligenza artificiale integrate nelle applicazioni SaaS?

Capiamo come utenti e agenti interagiscono con i modelli di intelligenza artificiale oggi?



Analizzare

Comprendi i pattern di rischio e l'esposizione dei dati legati all'uso dell'AI

Non tutti i dati hanno lo stesso valore. Questo principio guida le Policy di sicurezza aziendale da tempo. Ma non è mai stato così importante come nell'era dell'AI, dove i team di sicurezza cercano di trovare il giusto equilibrio tra accelerare l'innovazione e controllare il rischio. Capire più a fondo come vengono usati gli strumenti di intelligenza artificiale e il tipo di dati in transito può aiutare le aziende a prendere decisioni più intelligenti e concentrare le risorse in modo più efficace.

Da valutare

Sappiamo quali tipi di dati vengono condivisi con gli strumenti di intelligenza artificiale?

Possiamo distinguere tra interazioni AI a basso rischio e ad alto rischio?

Siamo in grado di individuare modelli che indicano rischi emergenti?

Applicare

Applicare controlli d’uso sicuro in tutte le interazioni con l'AI

L'approccio *zero trust* alla sicurezza si basa sul fornire l’accesso a seconda del contesto. Concedere l'accesso giusto diventa più complicato con l'AI, dal momento che gli strumenti potrebbero involontariamente fornire informazioni riservate a un collega che interroga uno strumento di AI aziendale. Oltre a questo c'è il continuo dispiegamento di agenti AI, che introducono nuovi vettori di attacco, comprese azioni autonome non sicure e percorsi ampliati per l'esfiltrazione dei dati.

Da valutare

Possiamo controllare l'uso dell'AI e l'accesso ai dati in base all'identità dell'utente/agente, alla sensibilità dei dati o al rischio?

I controlli sono coerenti tra i diversi strumenti e ambienti di intelligenza artificiale?

I nostri modelli di intelligenza artificiale privati sono protetti da tentativi di *jailbreak* o di ingegneria *prompt* dannosa?

Governare

Garantire un uso dell'AI conforme, tracciabile e gestito in modo responsabile

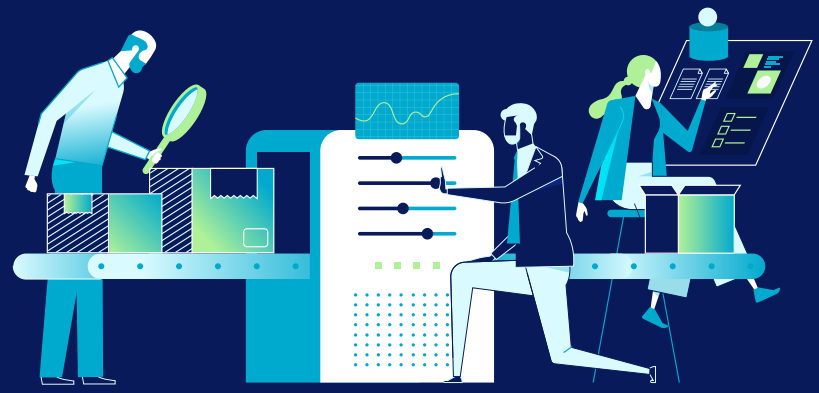
I professionisti della sicurezza sanno che la conformità agli standard del settore è fondamentale. Ma gli standard dell'AI si evolvono di continuo per stare al passo con la tecnologia, quindi è importante adeguare di conseguenza le politiche di sicurezza e mantenere sempre tracciati di controllo chiari. Questo è tassativo in settori come i servizi finanziari e l'assistenza sanitaria, dove la regolamentazione è fondamentale per le attività.

Da valutare

Possiamo dimostrare come è regolamentato oggi l'uso dell'AI?

Abbiamo auditabilità e tracciabilità nelle interazioni con l'AI?

Le responsabilità per l'uso dell'AI sono definite in modo chiaro?



Focus: per saperne di più sull'approccio di Netskope alla AI Security, leggi qui.

A proposito di Netskope

Netskope, leader nella sicurezza e nelle reti moderne per l'era del cloud e dell'AI, soddisfa le esigenze dei team di sicurezza e networking fornendo accesso ottimizzato e sicurezza in tempo reale in base al contesto per persone, dispositivi e dati ovunque. Migliaia di clienti, tra cui più di 30 nella Fortune 100, si affidano alla piattaforma Netskope One, al suo Zero Trust Engine e alla sua potente rete NewEdge per ridurre i rischi e ottenere massima visibilità e controllo su applicazioni cloud, AI, SaaS, Web e private che offrono sicurezza e prestazioni accelerate senza compromessi.

netskope

Vuoi saperne di più?

Chiedi una demo