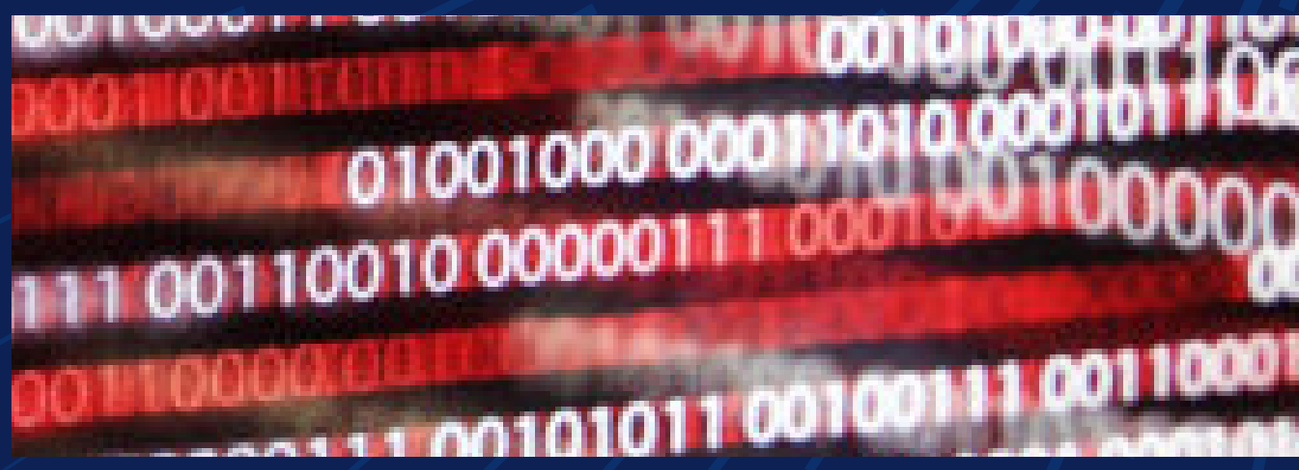
I miti della sicurezza informatica:

# sfatare i luoghi comuni sulla sicurezza dell'AI



L'AI sta trasformando tutti i settori ma, quando si parla di come proteggerla, molte organizzazioni cadono vittima di luoghi comuni che fanno apparire le misure di sicurezza più complesse di quanto siano in realtà. La verità? Per la protezione dei sistemi di AI non si deve partire da zero: l'applicazione dei tradizionali principi di sicurezza informatica alle sfide specifiche dell'AI è già un'ottima base.

Noi di Dell Technologies comprendiamo l'architettura su cui si fonda l'AI e possiamo aiutarti ad adattare le tue soluzioni attuali a questo nuovo framework. Sfatiamo i luoghi comuni più diffusi sulla sicurezza dell'AI e scopriamo la verità su come proteggere i sistemi in modo efficace.

## Luogo comune 1: "I sistemi di AI sono troppo complessi per essere protetti."

**Verità:** è vero che l'AI crea nuovi rischi per la sicurezza informatica, come gli attacchi di prompt injection, la manipolazione dei dati e la divulgazione di informazioni sensibili, solo per citarne alcuni. Inoltre, i sistemi di AI agentica presentano una superficie di attacco più ampia, che può essere sfruttata per manipolare i risultati o eseguire l'escalation dei privilegi.

Detto questo, sebbene sia fondamentale riconoscere queste vulnerabilità e implementare misure di sicurezza per proteggere i sistemi di AI sia dalle minacce tradizionali sia da quelle specifiche dell'AI, i rischi possono essere gestiti e i modelli di AI possono essere messi in sicurezza. È importante tenere presente che i sistemi di AI richiedono grandi quantità di dati di input e producono notevoli quantità di dati di output. Ciò significa che la protezione dei dati diventa un punto nevralgico della strategia di sicurezza, insieme a:

- Principi Zero Trust, ad esempio gestione delle identità, accesso basato sui ruoli e verifica continua.
- Test di penetrazione regolari e gestione delle vulnerabilità per identificare i punti deboli.
- Registrazione e audit per convalidare gli input e gli output dei dati

## Luogo comune 2: "Nessuno degli strumenti disponibili riuscirà a proteggere l'AI."

**Verità:** per proteggere l'AI non serve partire da zero, ma lavorare in modo più intelligente con gli strumenti già disponibili. La maggior parte degli strumenti di sicurezza informatica esistenti può essere adattata per proteggere efficacemente i sistemi di AI. In ultima analisi, l'AI è solo un altro carico di lavoro nel tuo arsenale a supporto del business, anche se con caratteristiche uniche. Le procedure di base per la sicurezza informatica, come la gestione delle identità, la segmentazione e il monitoraggio delle reti, la protezione degli endpoint e la tutela dei dati, sono essenziali anche per la sicurezza degli ambienti di AI. La chiave è adattare questi processi per affrontare le sfide specifiche dell'AI, come la protezione dei dati di addestramento, la difesa degli algoritmi e la riduzione di rischi quali gli input antagonisti.

Una difesa solida inizia con una buona igiene informatica, come l'applicazione di patch ai sistemi, il controllo degli accessi e la gestione delle vulnerabilità. Il fattore decisivo è la personalizzazione di tali processi per affrontare i rischi specifici dell'AI. Con strategie incentrate sull'AI integrate nell'attuale approccio alla sicurezza e con gli strumenti giusti, la sicurezza dell'AI diventa gestibile ed efficace.

Tuttavia, è importante sottolineare che l'aggiornamento dell'hardware può svolgere un ruolo cruciale nella lotta agli attacchi informatici. Ad esempio, i moderni AI PC forniscono una solida prima linea di difesa contro un importante vettore di attacco: gli endpoint. Con la fine del supporto per Windows 10, i PC obsoleti diventano un rischio. Inoltre, Windows 11 richiede Trusted Platform Module (TPM) versione 2.0, un chip di sicurezza che supporta la crittografia, l'avvio sicuro e la protezione contro gli attacchi al firmware. Molti PC meno recenti non dispongono del modulo TPM o supportano solo una versione precedente. Dell offre AI PC commerciali sicuri, che integrano queste funzionalità ottimizzate.

Lo stesso vale per l'infrastruttura AI come server e storage. Dell AI Factory include hardware ottimizzato per la sicurezza dell'AI, oltre a una serie di funzionalità di protezione integrate, ad esempio supply chain sicura, immutabilità dei dati, isolamento e crittografia.

## Luogo comune 3: "La sicurezza dell'AI riguarda solo la protezione dei dati."

**Verità:** la sicurezza dell'AI va oltre la protezione di base dei dati e abbraccia l'intero ecosistema AI, inclusi modelli, API, output, sistemi e dispositivi. Man mano che l'AI diventa più integrata nelle applicazioni critiche, aumentano anche i rischi associati al suo uso improprio o al suo sfruttamento. Senza solide misure di sicurezza, i modelli di AI possono essere manomessi per generare output dannosi o fuorvianti, le API possono essere sfruttate per ottenere accesso non autorizzato a sistemi sensibili e gli output possono, involontariamente, rivelare informazioni private o riservate.

Una sicurezza dell'AI completa richiede un approccio multilivello. Ciò include la protezione dei modelli da attacchi antagonisti che tentano di manipolare i dati di input per ingannare i sistemi di AI, la protezione delle API con metodi di autenticazione avanzati per impedire l'utilizzo non

autorizzato e **il monitoraggio continuo degli output** per individuare modelli anomali o sospetti che potrebbero suggerire un attacco o un malfunzionamento. Una sicurezza efficace dell'AI non garantisce solo l'integrità e l'affidabilità dei sistemi di AI, ma aumenta anche la fiducia di utenti ed entità interessate grazie alla riduzione dei rischi legati a usi dannosi o a conseguenze indesiderate.

## Luogo comune 4: "L'AI non ha bisogno di supervisione umana."

**Verità:** la governance e la supervisione umana sono fondamentali per garantire che i sistemi di AI funzionino in modo etico, prevedibile e in linea con i valori umani. I sistemi di AI avanzati, in particolare l'AI agentica dotata di capacità decisionali autonome, introducono sfide uniche che richiedono solide misure di sicurezza. Senza un'adeguata supervisione, questi sistemi potrebbero discostarsi dagli obiettivi previsti o presentare comportamenti indesiderati potenzialmente rischiosi.

Per risolvere questo problema, è essenziale stabilire confini chiari, implementare meccanismi di controllo a più livelli e garantire un coinvolgimento umano continuo nei processi decisionali critici. Audit regolari, trasparenza nelle operazioni di AI e test approfonditi possono aumentare ulteriormente la responsabilità e la fiducia, contribuendo a prevenire l'uso improprio e promuovendo il deployment responsabile delle tecnologie di AI.

## Best practice per rafforzare la sicurezza dell'AI

**Per colmare le lacune di sicurezza specifiche dell'AI, le organizzazioni devono adottare un approccio proattivo e strategico. Di seguito sono illustrate 10 best practice per la protezione dei sistemi AI:**

**Architettura di sicurezza a più livelli:**
Usa segmentazione, firewall e autenticazione avanzata per proteggere l'infrastruttura, il software e i dati a ogni livello.

**Protezione della supply chain:**
Implementa un solido programma di gestione dei fornitori. Controlla i vendor e i componenti di terze parti, convalida l'integrità e affidati a codice firmato per evitare vulnerabilità nel ciclo di vita dello sviluppo dell'AI.

**Protezione dei dati e dei modelli di addestramento:**
Proteggi i sistemi da dati contaminati, input antagonisti e altre minacce monitorando l'integrità dei dati e applicando solidi strumenti di convalida.

**Rafforzamento dei controlli degli accessi:**
Applica i principi del privilegio minimo, implementa il controllo degli accessi basato sui ruoli (RBAC), ruota regolarmente le credenziali e controlla le autorizzazioni per impedire l'accesso non autorizzato.

**Protezione delle API:**
Usa protocolli di autenticazione avanzati (come OAuth 2.0), applica la crittografia HTTPS e aggiorna regolarmente le API per risolvere le potenziali vulnerabilità.

**Monitoraggio e convalida degli output AI:**
Usa il rilevamento delle anomalie, la registrazione e gli avvisi per rilevare la presenza di modelli anomali o comportamenti dannosi negli output AI.

**Pianificazione della resilienza:**
Esegui regolarmente il backup dei dati e verifica i piani di ripristino di emergenza per ridurre al minimo il downtime e garantire un ripristino rapido in caso di violazione.

**Implementazione di una solida crittografia:**
Crittografa i dati sensibili inattivi e in transito utilizzando algoritmi avanzati e gestisci e ruota a cadenza regolare le chiavi di crittografia in modo sicuro.

**Esecuzione a cadenza regolare di audit di sicurezza e test di penetrazione:**
Controlla spesso i sistemi alla ricerca di vulnerabilità e utilizza i test di penetrazione per individuare i rischi prima che possano essere sfruttati.

**Formazione del personale sulle best practice per la sicurezza dell'AI:**
Offri regolarmente corsi di formazione ai team sullo sviluppo sicuro, sul riconoscimento delle minacce e sul mantenimento di solide procedure di sicurezza per prevenire le violazioni.



DELL Technologies

## Proposta di valore di Dell: soluzioni pratiche per la sicurezza dell'AI.

La sicurezza dell'AI può sembrare complessa, ma in realtà è più gestibile di quanto si possa pensare. La verità? Proteggere l'AI non è così diverso da proteggere i carichi di lavoro esistenti: si tratta di comprendere l'architettura e applicare le strategie giuste. Ed è qui che entra in gioco Dell Technologies.

Semplifichiamo l'approccio alla sicurezza dell'AI usando le soluzioni disponibili e integrandole senza problemi nelle architetture incentrate sull'AI. Gestiamo problemi quali gli attacchi di prompt injection, l'uso improprio delle API e gli attacchi antagonisti senza la necessità di rivedere integralmente l'infrastruttura.

Grazie alle sue competenze, Dell contribuisce a sfatare i luoghi comuni sulla sicurezza dell'AI e a mostrare concretamente quanto sia realizzabile. Se sei agli inizi del tuo percorso verso l'AI o se intendi consolidare le tue difese, Dell può aiutarti a proteggere gli investimenti, mettere in sicurezza i sistemi e costruire un futuro digitale resiliente, in modo affidabile ed efficace. Semplifichiamo insieme la sicurezza dell'AI.

## Prodotti e soluzioni Dell utili

| Soluzione consigliata Dell | Descrizione |
|---|---|
| Dell AI Factory | Dell AI Factory protegge i carichi di lavoro AI tramite una supply chain sicura, garantendo l'affidabilità dell'infrastruttura dallo sviluppo al deployment. Grazie a funzionalità quali l'immutabilità, l'isolamento e la crittografia dei dati, protegge modelli e dataset sensibili, contrasta le minacce informatiche e permette di eseguire operazioni di AI scalabili, efficienti e senza interruzioni in ambienti dinamici e basati sui dati. |
| Cyber-resilienza | PowerProtect protegge i carichi di lavoro AI con funzionalità avanzate come l'immutabilità e l'isolamento, garantendo l'integrità e la protezione dei dati contro le minacce informatiche. Offre crittografia end-to-end e rilevamento delle anomalie, oltre alla possibilità di ripristinare rapidamente i sistemi per ridurre al minimo il downtime. |
| Dell Trusted Workspace (Sicurezza degli endpoint) | Una combinazione di funzionalità Add-On integrate e opzionali progettate per proteggere gli AI PC commerciali e i carichi di lavoro AI eseguiti su di essi. Realizzate con procedure della supply chain protette, le funzionalità integrate includono SafeBIOS e SafeID con TPM. Gli Add-On opzionali includono Secured Component Verification, SafeID con ControlVault e i software dei partner CrowdStrike e Absolute per ottimizzare la sicurezza dell'ambiente di lavoro. |
| AI Security Advisory Services | Una suite di servizi che può aiutarti a sviluppare e implementare una strategia di sicurezza dell'AI completa. Sono inclusi servizi di consulenza, vCISO di AI e pianificazione della sicurezza dei dati. |
| Operazioni di sicurezza gestite per l'AI | Offre una visibilità profonda di tutto lo stack per rilevare le minacce e rispondere rapidamente. Le funzionalità includono Managed Detection and Response, AI Guard gestito, test di penetrazione per l'AI e Incident Response and Recovery Services. |
| Integrazione del software di sicurezza | Progetta, installa e configura strumenti di sicurezza che proteggono la gestione degli accessi, le applicazioni, le reti, i cloud e altro ancora. |

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi su **dell.com/cybersecuritymonth**