SCHEDA TECNICA

Digitale Fraud Defender

Protegge la verifica dell'identità digitale dalle frodi avanzate basate sull'AI

La verifica del documento di identità (IDV), il processo che garantisce che una persona sia in possesso di un documento di identità valido rilasciato dal governo, è un forte indicatore che la persona è reale e legittima. Tuttavia, l'intelligenza artificiale generativa (GenAI) ha reso molto più economico e semplice commettere forme sofisticate di frode, come l'introduzione di immagini false nei flussi di lavoro dei processi di verifica o la creazione e l'utilizzo di identità sintetiche generate con i deepfake.

Oggi, le aziende devono combinare l'IDV con il rilevamento digitale multilivello per affrontare i vettori di frode avanzati indotti dall'AI.

Digital Fraud Defender di Mitek è progettato per proteggere il processo di verifica dell'identità dalle moderne tecniche di frode, come deepfake, attacchi injection e attacchi ai template digitali. Questa soluzione consente alle aziende di farsi trovare pronte contro le nuove minacce che emergono costantemente.

A differenza di altre tecnologie di rilevamento di deepfake e di rilevamento degli attacchi injection, *Digital Fraud Defender* È progettato per esaminare le prove dal momento dell'acquisizione, durante il processo e durante l'esecuzione di confronti. Inoltre, l'approccio avanzato di Mitek valuta più tipi di attacchi, utilizzati singolarmente o in combinazione, evitando di fare affidamento su un'unica fonte o punto di errore.

Rilevamento digitale delle frodi a più livelli:

Protezione contro gli attacchi injection

- Rilevamento presenza telecamere virtuali
- Rilevamento dell'uso di telecamere virtuali
- Rilevamento di risoluzioni sospette
- Rilevamento di frame doppi
- Rilevamento di discrepanze tra l'acquisizione e l'evidenza nel server

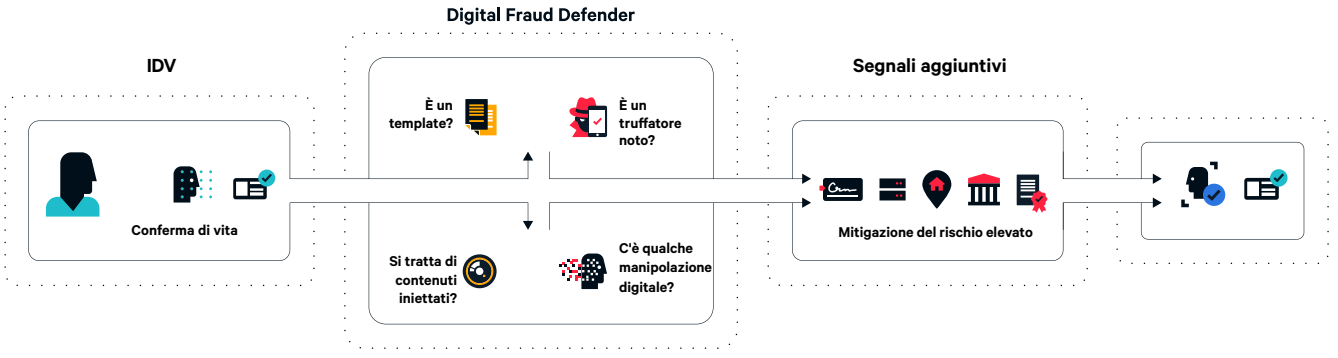
Protezione contro gli attacchi con Template

- Controllo della velocità facciale (ricorrenza delle immagini)
- Controllo della galleria (confronto con gallerie di noti truffatori)
- Valutazione della manipolazione dei contenuti digitali

Protezione contro gli attacchi deepfake

- Rilevamento della filigrana generato dall'AI
- Rilevamento di contenuti sintetici e motori di generazione di contenuti
- Verifica dei fondi documentali negli attacchi organizzati *(ring attacks)*

Flusso di lavoro di verifica dell'identità



Digital Fraud Defender Workflow

È in gioco il futuro della fiducia online

Il mancato rilevamento delle frodi basate su GenAI potrebbe avere gravi conseguenze per le aziende che non sono preparate per combatterlo. L'onboarding digitale dei clienti potrebbe essere interrotto, i processi di verifica a più livelli potrebbero essere aggirati e le sanzioni normative o di conformità, insieme all'accelerazione del tasso di abbandono dei clienti, potrebbero avere conseguenze molto reali.

Con l'aumento delle vulnerabilità alla velocità dell'AI, la necessità è chiara: ora è il momento di implementare soluzioni di verifica dell'identità digitale più resilienti, avanzate, adattive e innovative come gli stessi malintenzionati.

L'ascesa dell'AI generativa

Secondo il *Deloitte Center for Financial Services*, le perdite dovute alle frodi legate all'AI generativa e ai deepfake potrebbero raggiungere **38 miliardi di euro entro il 2027**, in contrapposizione agli **11 miliardi del 2023**. Soltanto nel settore fintech, si prevede che i deepfake aumenteranno del **700% entro il 2031**.

Digital Fraud Defender è un insieme di funzionalità avanzate di prevenzione delle frodi che utilizza una potente AI per rilevare le manipolazioni digitali durante il processo di verifica dell'identità. Offre:

Rilevamento olistico delle frodi digitali
Protegge dagli attacchi abilitati con AI, rilevando deepfake, scambi facciali, morfologia, telecamere virtuali, identità sintetiche, modelli di prove ripetuti e altro ancora.

Difesa contro più vettori di attacco
Risponde efficacemente agli attacchi individuali o combinati.

Identificazione più rapida delle frodi digitali organizzate
Rileva i tentativi di frode ricorrenti da parte di malintenzionati noti o truffe ripetute e risponde più rapidamente ai nuovi attacchi basati su template.

Preparazione verso le minacce emergenti
Progettato con un approccio a più livelli, accelera la capacità di riconoscere e neutralizzare rapidamente nuovi attacchi.

La nuova generazione di rilevamento delle frodi d'identità, solo con Mitek

Sviluppato come un insieme di funzionalità all'interno della Mitek Identity Verification Platform (MiVIP), ***Digital Fraud Defender*** si basa sull'esperienza di Mitek in prima linea nella verifica dell'identità, nell'autenticazione, nella biometria, nell'acquisizione delle immagini e nel rilevamento delle frodi.

I componenti fondamentali dell'AI e *Machine Learning* (ML) che guidano *Digital Fraud Defender* rispecchiano il rigore dei **40 anni di storia Mitek** nell'innovazione a livello bancario. Con questa soluzione, le aziende possono affrontare con sicurezza il futuro delle frodi digitali.

Combatti l'AI con l'AI

Contromisure per vettori specifici di minaccia

La nostra esperienza in materia di sicurezza informatica, gli ampi set di dati e i test rigorosi dei nostri ingegneri di machine learning, che adattano i nostri modelli per affrontare specifici vettori di minaccia, garantendo che le nostre reti neurali imparino a rilevare le tracce uniche di ogni nuovo attacco.

Architettura tecnologica modulare e altamente adattabile

Un design iterativo e flessibile ci consente di rispondere alle minacce emergenti con una velocità e una precisione senza precedenti, implementando gli aggiornamenti senza la necessità di una ricalibrazione completa o di rilasci formali.

Ampia copertura nei confronti di contenuti artificiali

I nostri modelli sono adattati per rilevare varie tecniche e manipolazioni digitali, come tecniche di diffusione, styleGAN, animazioni di immagini, scambi di volti, morfologia, iniezioni sui social network, chipfake e altre manipolazioni digitali.

Modelli di AI preparati su set di dati accuratamente selezionati

La selezione dei set di dati e la preparazione specifica dei nostri modelli garantiscono risultati precisi e adattati alle esigenze specifiche dei clienti. I nostri modelli sono equi ed efficaci e sono stati monitorati da laboratori terzi indipendenti per garantire che siano imparziali.

Analisi avanzata dei flussi video

Ispezione approfondita, fotogramma per fotogramma, delle prove video per garantire l'integrità dei dati inviati e prevenire la manomissione.

Laboratorio interno di deepfake e generazione di dati fraudolenti

I nostri team interni di intelligenza artificiale e scienza dei dati generano deepfake avanzati e altri contenuti fraudolenti, consentendoci di valutare a fondo le nostre soluzioni rispetto a scenari di frode del mondo reale e di muoverci alla stessa velocità con i cambiamenti tecnologici.

Inizia ora!

Per ulteriori informazioni su come *Digital Fraud Defender* può aiutare la tua azienda a difendersi in questa nuova era di frodi di identità digitale, Contattaci.