Mitek

DATA SHEET

Digital Fraud Defender

Protect digital identity verification from advanced, AI-powered fraud.

While identity document verification (IDV), the process of ensuring an individual has a valid, government-issued ID, is a very strong indicator that they are indeed a real and legitimate person, Generative AI (GenAI) has made it significantly cheaper and easier to commit sophisticated forms of fraud, like injecting fake images into the IDV workflow or creating and using deepfake-produced synthetic identities. Today, organizations need IDV plus layered digital detection for advanced, AI-powered fraud vectors.

Digital Fraud Defender from Mitek is designed to safeguard the identity verification process from modern fraud techniques like deepfakes, injection attacks, and digital template attacks, helping to future proof your organization from emerging threat vectors.

Unlike other deepfake and injection attack detection technologies, Digital Fraud Defender is designed to examine evidence from the point of capture, its transit state, and at the point of comparison. In addition, Mitek's advanced approach tests for multiple types of attacks, whether used individually or in combination, to avoid relying on a single source or point of failure.

Multi-layered digital fraud detection

Injection attack protection

- Virtual camera presence detection
- Virtual camera usage detection
- Suspicious resolution detection
- Duplicated frames detection
- Capture vs. server evidence mismatch detection

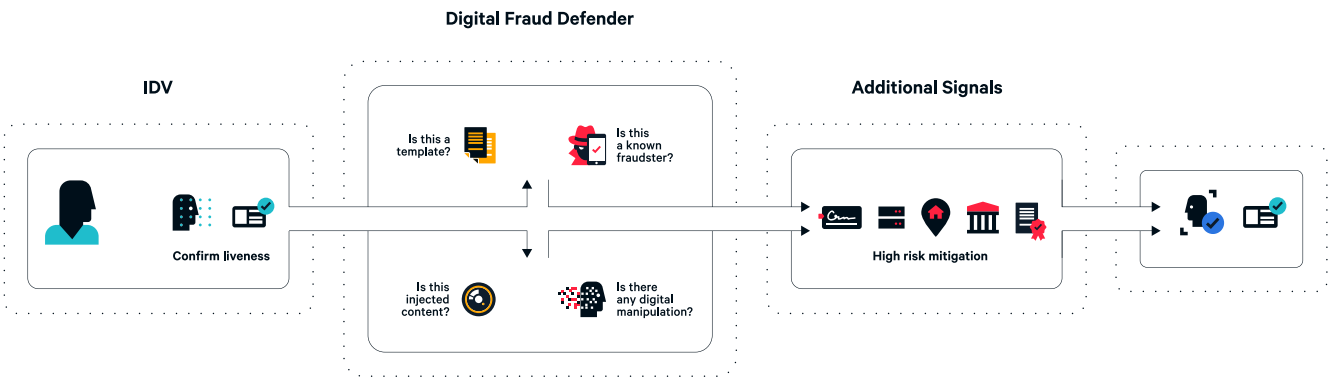
Template attack protection

- Face velocity (image recurrence) checks
- Gallery review (known fraudster gallery comparison)
- Ring attack background checks (document backgrounds)

Deepfake attack protection

- Digital content manipulation assessment
- AI-generated watermark detection
- Synthetic content and content engine detection

Identity Verification Workflow

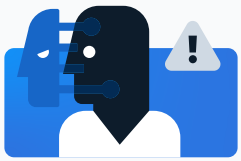


Digital Fraud Defender Workflow

The future of online trust is at stake

Failing to detect GenAI-based fraud could have sweeping consequences for organizations who are not prepared to combat it. Digital onboarding can be disrupted. Step-up verification processes can be circumvented. Heavy compliance or regulatory penalties and accelerated customer churn can be very real consequences.

With vulnerabilities escalating at the speed of AI, the need is clear. Now is the time for more resilient digital identity verification solutions that are as advanced, adaptive, and innovative as bad actors.



GenAI is booming

Fraud losses related to **generative AI and deepfakes could reach $40 billion** in the United States by 2027—up from $12.3 billion in 2023, according to the Deloitte Center for Financial Services. In the fintech sector alone, **deepfakes are expected to increase by 700%** by 2031.

Digital Fraud Defender is a suite of advanced fraud prevention capabilities that uses powerful AI to uncover digital manipulation across the identity verification process. **It delivers:**

Holistic digital fraud detection.
Defend against multiple attack vectors whether used alone or in combination.

Protection from AI-enabled attacks.
Catch deepfakes, face swaps, morphing, virtual cameras, synthetic identities, repeated evidence patterns and more.

Faster identification of organized digital fraud attempts.
Spot recurring fraud attempts from known bad actors or recurring scams—and respond faster to new template attacks.

Futureproofing against emerging threats.
Architected with a multi-layered approach to detection, it accelerates the ability to swiftly recognize and neutralize new attacks.

The next generation of identity fraud detection, only from Mitek

Delivered as a suite of capabilities through the Mitek Verified Identity Platform (MiVIP), Digital Fraud Defender was built on Mitek's experience on the front lines of identity verification, authentication, biometrics, image capture, and fraud detection. The foundational AI and Machine Learning (ML) components that power Digital Fraud Defender reflect the rigor of Mitek's 40 year history of banking-grade innovation.

Fight AI with AI

Countermeasures for specific threat vectors.
Cybersecurity expertise, vast data sets, and rigorous testing by our ML engineers train our models for specific threat vectors, ensuring our neural networks learn to detect the unique artifacts of each new attack.

AI models trained by carefully curated data sets.
Selecting data sets and curated training of our own models supports accuracy and precise results tailored to customer needs. Our models are fair and effective and have been tested by third-party independent labs to ensure they are unbiased.

Modular and highly adaptive technology architecture.
An iterative, flexible design allows us to respond to emerging threats with unmatched speed and precision, implementing updates without the need for full recalibration or formal releases.

Advanced video stream analysis.
Deep, frame-by-frame inspection of video evidence ensures the integrity of the submitted artifacts and prevents data compromise.

Broad coverage of artificial content.
Our models are trained to detect diffusion techniques, styleGANs, image animations, face swaps, morphs, social media injections, chipfakes, or other digital manipulations.

Internal deepfake and data generation lab.
Our in-house artificial intelligence and data science teams generate advanced deepfakes and other fraudulent content, allowing us to thoroughly evaluate our solutions against real world fraud scenarios and progress our solutions at the speed of technological change.

Get started

To learn more about how Digital Fraud Defender can help your enterprise defend against a new era of digital identity fraud, visit miteksystems.com/gen-ai-identity-fraud