2026 Injection Attack Detection Market Report & Buyer's Guide

by Biometric Update and Goode Intelligence

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Industry Profiles

2026 IAD Market Report and Buyer's Guide

Injection Attack Detection (IAD) has become a critical component of digital identity security as organizations confront AI-driven fraud attacks. Biometric Update and Goode Intelligence have therefore partnered on a report examining the technologies, standards and market forces shaping the injection attack detection market.

Injection attacks occur when fraudsters bypass biometric capture devices and insert manipulated or synthetic content directly into digital identity workflows. Unlike traditional presentation attacks that rely on physical artifacts such as masks, printed photos or replay devices, injection attacks exploit software, networks, virtual cameras, emulators and AI-generated media to compromise biometric systems at scale.

The growth of remote onboarding, biometric authentication and generative AI has expanded the attack surface for digital identity fraud. As organizations increasingly rely on facial biometrics, liveness detection and identity verification, injection attack detection is becoming an essential layer of identity assurance and fraud prevention.

IAD works alongside liveness detection, Presentation Attack Detection (PAD) and deepfake detection to protect biometric capture and authentication processes. It is designed to identify attempts to manipulate camera feeds, inject synthetic media, exploit virtual devices or tamper with identity verification workflows before fraudulent content reaches a biometric matching system.

This Biometric Update / Goode Intelligence report explains IAD, examines available technologies and helps buyers evaluate solution providers.

The study also investigates the global market for IAD technologies, including adoption drivers, market analysis, standards developments, vendor activity and three-year forecasts for attack attempts and detection checks. The accompanying buyer's guide provides practical advice for evaluating suppliers and the capabilities needed to defend against AI-enabled identity fraud.

About Biometric Update and Goode Intelligence

This study has been created by a partnership bringing together Biometric Update and Goode Intelligence to produce analytical market reports stakeholders can use to make informed strategy, product and technology procurement choices.

Reports produced by the partnership are based on analysis of recent transactions and trends in the biometrics market, reviews of the regulatory, standards-development and competitive landscapes, and feedback from key insiders in each given area of focus.

Biometric Update is the world's leading source for daily news, opinion and insight into biometrics and digital identity.

Goode Intelligence is the world's leading independent biometrics market analyst and consulting firm, providing quality advice to global decision makers in business and technology.

Executive Summary

Injection attack detection (IAD) is a primary method of defending against deepfake-driven fraud, particularly in systems that rely on face biometrics. Used alongside presentation attack detection (PAD), injection attack detection helps protect digital identity systems from sophisticated spoofing or impersonation attacks. Injection attack detection is therefore deployed by organizations that use biometrics for digital remote or unsupervised user onboarding and authentication.

The rapid rise of generative AI allows fraudsters to create highly realistic deepfake videos and voice clones, which can be injected directly into systems to bypass basic fraud checks.

This report forecasts annual injection attack attempts will grow from 122 million in 2026 to more than 301 million by 2028, driving over 4 billion IAD checks annually. To counteract the rising threat from injection attacks, this study investigates the best methods to detect and prevent injection attacks, drawing on the collaborative experience of some of the industry's leading experts and technology suppliers.

IAD solutions are predominantly sold as part of liveness detection and deepfake detection solutions, as part of anti-fraud measures in biometric identity and authentication systems to answer these critical questions when a person is onboarding or authenticating; is the person present, genuine, alive, and not a spoof or synthetically generated.

The Injection Attack Detection Market Report & Buyer's Guide analyzes this rapidly evolving market, outlining technology approaches, vendor offerings, and why IAD has become a critical requirement for high-value biometric use cases such as financial onboarding.

As both an important anti-fraud defense and a new technology, IAD is an emerging market. Many businesses must improve their understanding of IAD and how it works to take advantage of the protection it provides against sophisticated fraud.

Injection attacks are changing the economics of biometric fraud. Where presentation attacks required physical artifacts such as masks, printed photos or replay devices, injection attacks allow fraudsters to scale attacks through software, virtual cameras, emulators and AI-generated media. As organizations increasingly rely on remote onboarding and biometric authentication, protecting the integrity of the capture pipeline has become as important as verifying the person in front of the camera.

Introduction to Injection Attack Detection

Injection attacks hijack a hardware device, media stream or piece of code and "inject" foreign content into the information feed. Imagine stealthily taking over a radio station's broadcast signal and pretending to be the deejay – then asking for listeners to wire them money. That's the basic concept behind injection attacks. But the specifics of this emerging threat are much more complex, and require a vigilant security posture. Injection attack detection (IAD) technologies and standards-based testing to evaluate them are still maturing. But these tools and technologies are evolving quickly to meet the threat.

Biometric injection attacks are a relatively new menace, in that they depend on the use of remote biometrics, especially for remote identity proofing or identity verification. These injection attacks exploit biometric features, most commonly face and voice, by replacing an authentic media feed with fake media created by a fraudster, often using generative AI. Unlike biometric presentation attacks that rely on physical methods like printed photos or masks, injection attacks exploit weaknesses in software, networks or hardware, which makes them more scalable. Voice cloning, spoofs, emulators, virtual cameras, and synthetic or manipulated identities are among the types of digital tools that are easier than ever to find, access and exploit for fraud.

In addition to hijacking live media feeds with spoofed faces and voices, fraudsters can use injection attacks to insert fake identity documents into onboarding and ID verification flows. In fact, faked identity documents have an even lower access threshold than realistic deepfaked people. Generative technologies can easily be used to perform face swaps on an identity document, or to switch out full or partial text inserted on textual fields.

The mechanics of biometric injection attacks require specific techniques for defense. The attack surface for injection attacks is anywhere between the biometric sensor and the orchestrator or integrator, or a biometric comparison component. That means the attack can occur in front of the app, within the app or after it, and that the delivery device itself is compromised along with the content. Because injection attacks can target cameras, a selfie – even a video selfie with liveness detection – is not sufficient to protect and secure identity proofing and verification processes.

As such, IAD is divided into defense against the attack method and the attack instrument. Examples of methods include camera anti-tampering mechanisms, session metadata analysis, code obfuscation, runtime application self-protection and mobile device emulator detection. Defense against attack instruments includes detection of replay attacks or automated artifacts and procedural controls, like introducing randomness or manual inspection.

Distinguishing IAD from Liveness and Deepfake Detection

As organizations confront AI-generated fraud and increasingly sophisticated biometric attacks, several adjacent technologies are often discussed together — including IAD, liveness detection and deepfake detection. While these technologies overlap in important ways, they address different threat vectors, operate at different layers of the authentication process and solve distinct security problems. Understanding those differences is becoming increasingly important as enterprises, governments and digital platforms build layered defenses against synthetic identity fraud and AI-enabled impersonation attacks.

Presentation attack detection

Liveness detection aims to determine whether or not an image or biometric sample provided for identity verification or authentication is of a real, living human. Traditionally, PAD protects against attacks that "present" a false biometric or spoof, such as a 3D silicon mask, or photos, videos and other fake artifacts, increasingly generated with AI tools. It is a primarily visual analysis. Liveness detection takes the concept further in its attempt to verify humanness, and may involve analyzing factors like blood flow or the cadence of speech.

Deepfake detection

Deepfake detection is looking at media content. It can analyze image or video frames for signs that the content might be products of face-swapping apps or other generative AI: subtle clues in pixel structure and lighting, or discrepancies between lip movement and mouth shape. Deepfakes can be deployed in injection attacks, but detecting them is not the same process as IAD, which monitors the integrity of the camera feed and signal.

In practice, organizations are increasingly deploying these technologies together as part of broader identity assurance architectures. PAD helps confirm that a real person is present, deepfake detection analyzes manipulated or synthetic media, while IAD focuses specifically on protecting the integrity of biometric capture and authentication pipelines from injected or tampered inputs. As AI-generated attacks become more scalable and sophisticated, the distinctions between these categories matter less in isolation than how effectively they work together within a unified trust and fraud defense stack.

Why IAD Matters Now

IAD has gone from an emerging technology to a critical business requirement for numerous organizations at a nearly unprecedented pace, due the convergence of three major trends in digital technology.

Remote onboarding has become a popular way for people and businesses to register for services, and app-based authentication of registered users has increased accordingly. This creates a dramatically larger digital attack surface for businesses just as the third trend, inexpensive and widely available generative AI, makes sophisticated fraud attacks much easier than ever before. Injection attacks are the vector of delivery for these sophisticated attacks.

Many businesses are caught between the need to expand their market reach and customer interactions through digital channels and the need to secure those interactions against novel threats that fraudsters can use to gain entry into the system as trusted users. All are dependent on digital trust. IAD is the technology that secures that trust.

The convergence of remote onboarding, generative AI and app-based authentication has dramatically expanded the attack surface for biometric fraud.

The Threat Landscape

Why Injection Attacks are Different

Injection attacks present a unique threat because they bypass the physical camera. That means they are attacking the authentication workflow after the point at which an initial security check usually happens. As such, nothing that primarily serves to recognize the face of a user for biometric authentication at the camera stage will work to stop injection attacks. If an authentication workflow was an amusement park, instead of trying to trick the gate agent to let them through (like presentation attacks), injection attacks parachute in, or sneak in under a loose fence.

Common Attack Vectors and Types

Software is the most common injection attack vector. **Virtual cameras** simulate a physical webcam; they replace the door (camera) to a video conference, live streaming platforms, or video chat services with a fake (virtual) one. For this reason, the technique is also sometimes called "camera spoofing." Users typically install virtual webcam software as a plug-in or standalone application, then select it as the video input source for the application they are targeting.

Device emulators are software or hardware that allows a system to imitate another device. A simple way to think of it is like a digital calculator, but for smartphones, tablets or other devices, recreating them and their functions digitally. Another example is online emulators of old computer game systems. Almost any type of device with connectivity can be emulated. Using an emulator, attackers can build a virtual copy of a physical device and replace it in the authentication flow. Compromised physical devices are another problem.

In a **replay attack**, attackers capture transmitted legitimate authentication or access control information, then retransmit it to gain unauthorized access, effectively using someone else's recorded credentials.

API manipulation is when attackers alter API requests to exploit application logic, or insert malicious code into input fields to change how an application behaves.

Synthetic document and media injection attacks use software to replace authentic documents with fakes, or legitimate media content with whatever a fraudster wants. With generative AI lowering the access barrier for creating realistic deepfakes and synthetic personas, it is possible to generate a synthetic identity and use biometric injection attack methods to hack it into media feeds.

Implications for Buyers

Because the threat overlaps different techniques and industries, it has created a fragmented threat landscape. Siloed security frameworks are further burdened by a fractured lexicon: vendors often use different terminology and focus on different attack classes, which, for a buyer of injection attack detection, can make product comparisons difficult.

The unique nature of injection attacks necessitates new questions buyers should ask when choosing a provider. Buyers should equip themselves with an understanding of the interconnectivity (and difference) between IAD, PAD liveness and device intelligence. Vendors should be transparent in explaining which attack classes their product covers, and whether they have subjected their product to independent testing.

Market Delivery Models for Injection Attack Detection

How Injection Attack Detection Reaches Buyers

Where does Injection Attack Detection (IAD) actually get sold, and who is selling it? The answer is more complex than it first appears. IAD has not yet matured into a standalone market in the same way as identity verification or Presentation Attack Detection (PAD). Moreover, the evolution of the security landscape means IAD is increasingly bundled into broader identity assurance, liveness detection, fraud prevention and authentication stacks – and rarely offered as a standalone product.

As a result, organizations looking to defend against deepfakes, virtual cameras, emulators and other software-based attacks are often purchasing IAD capabilities indirectly through larger platforms, rather than procuring dedicated IAD products. This makes IAD difficult to isolate as a distinct market segment.

While standalone vendors exist, and other biometrics firms are beginning to explicitly feature IAD in their product offerings, the IAD ecosystem currently consists of several overlapping provider categories, and buyers may have difficulty simply finding IAD, or knowing where to look. Yet understanding how IAD reaches buyers – and where vendors are incorporating it – is critical to understanding both the current market and its future growth trajectory.

The following categories illustrate the primary routes through which organizations encounter and procure injection attack detection capabilities today. These categories are not mutually exclusive. In many cases, the same vendor may deliver IAD through multiple channels simultaneously. A company may appear as a liveness provider, identity verification platform, fraud orchestration vendor and government identity supplier depending on the deployment environment. This overlap reflects the broader convergence occurring across digital identity, fraud prevention and trust infrastructure markets.

» **Vendors increasingly position IAD not as an isolated capability, but as part of a broader trust and fraud prevention stack.**

Standalone and Modular IAD Offerings

Specialized, standalone IAD capabilities represent the most direct route to targeted injection attack protection. While the broader market frequently bundles these features into all-in-one identity verification suites, a distinct

but limited class of providers offers IAD as a decoupled, modular layer.

Identity security providers and enterprise developers integrate these standalone features to secure the integrity of biometric capture and authentication pipelines against software-based attacks like virtual cameras, emulators, media injection, session manipulation, and synthetic content insertion. Buyers typically look for these advanced, standalone IAD modules when baseline presentation liveness, identity verification, or fraud platforms fail to stop sophisticated attacks, or when regulators, auditors, and internal security teams demand independent validation of injection resilience without replacing their entire existing biometric infrastructure.

Organizations often evaluate these independent layers after discovering residual exposure to software-based attacks that standard onboarding systems were not designed to address. These high-assurance, modular IAD capabilities are most commonly adopted by banks, fintechs, government agencies, and identity providers operating in elevated fraud environments.

Representative providers delivering this advanced, standalone, or modular IAD protection include: Facephi, ID-Pal, Incode, Innovatrics, Keyless, Mitek, Mobbeel, Oz Forensics, ROC, Unissey, and Youverse.

Liveness Detection with Integrated IAD

For many organizations, liveness detection vendors are the primary route through which IAD is acquired. The transition from PAD to IAD often occurs within an existing liveness deployment rather than through an independent procurement process.

As fraud attacks evolved from physical presentation attacks to software-based injection attacks, liveness providers have expanded their core architecture beyond traditional PAD to include deepfake detection, device integrity checks and injection attack detection.

This channel is particularly important because many organizations still view fraud primarily as a presentation attack problem. As a result, injection attack protection is increasingly being bundled into liveness offerings rather than procured separately. In many cases, buyers seeking stronger liveness detection capabilities may not realize they are also purchasing IAD functionality.

Representative vendors include BioID, FaceTec, Identy, Incode, iProov, Jumio, Microblink, Oz Forensics, Shufti, Thales, and Yoti.

Identity Verification with Integrated IAD

Identity verification platforms represent one of the fastest-growing delivery channels for IAD deployment. Driven by the standardization of remote onboarding across banking, telecommunications, gaming, digital marketplaces, and e-government services, identity verification providers are under pressure to secure the entire onboarding journey against AI-enabled fraud.

For many buyers, the first encounter with injection attack detection occurs during an identity verification procurement rather than through a dedicated fraud or cybersecurity initiative. As a result, IAD is increasingly embedded within document verification, biometric matching, liveness detection and broader, onboarding orchestration workflows.

This trend is particularly visible in high-compliance sectors where identity verification serves as the front line of defense against synthetic identities, account opening fraud and deepfake-enabled impersonation.

Vendors active in this category include AU10TIX, Entrust, Facephi, GBG, Innovatrics, ID-Pal, Mitek, Ondato, Persona, Prove, Regula, Signicat, Trulioo, Unico, Veriff, and Yoti.

Fraud Prevention and Risk Platforms

Fraud orchestration vendors are increasingly integrating deepfake detection, liveness, and IAD into broader fraud decisioning systems. Fraud prevention and risk platforms mitigate injection threats very differently based on their specific product focus.

Sardine and BioCatch approach IAD from the device health and continuous behavioral level. Feedzai, SEON, and Authsignal serve as orchestration engines, aggregating third-party IAD via ecosystem integrations and routing risk signals through dynamic, no-code rule workflows to automate step-up verification.

Incognia approaches identity trust from a spatial perspective rather than a visual one, cross-referencing a device's video session with highly precise location signals and mobile motion sensors. Similarly, Prove mitigates injection vectors out-of-band by leveraging real-time mobile network intelligence and cryptographic device-possession signals to stop automated emulation pipelines before they can execute.

Government and Border Ecosystems

The IAD market for government, immigration, and border ecosystems is undergoing a significant architectural shift. Historically, border control focused on physical PAD. However, the rise of sovereign digital IDs, mobile passports and remote visa onboarding has forced governments to secure underlying data pipelines. In government ecosystems, an injection attack can involve a state-sponsored actor or criminal syndicate feeding synthetic content directly into national identity, immigration or border systems.

The government IAD market operates across two distinct environments: remote citizen onboarding and visa control via mobile apps – the higher

risk for injection attacks – and physical border checkpoints and airport e-Gates. As governments move toward digital wallets, remote onboarding and reusable digital credentials, IAD is becoming an increasingly important control for protecting national identity infrastructure from synthetic and injected content.

Paravision is a major player in the government, border control, and defense-grade biometric sectors, approaching the problem from a highly specialized computer vision and pure math perspective. IDEMIA Public Security is a dominant player in global government ID and border crossing infrastructure. Other firms providing IAD services to governments include Keyless, Incode, iProov, and Regula.

The absence of a clearly defined standalone IAD procurement market should not be mistaken for weak demand. Rather, the technology is being absorbed into adjacent identity, fraud and trust categories as organizations race to secure remote digital interactions against increasingly sophisticated AI-driven attacks.

The Shift Toward Integrated Platforms

The examples above illustrate that IAD is becoming a required capability across multiple identity, fraud and authentication markets, and that it is reaching those markets through multiple channels rather than emerging as a standalone procurement category. Dedicated IAD providers continue to advance the technology, but much of the current adoption is occurring through liveness detection, identity verification, fraud prevention and government identity platforms.

This overlap is reshaping the competitive landscape. Vendors increasingly position IAD not as an isolated capability, but as part of a broader trust and fraud prevention stack.

The market for biometric anti-spoofing technologies has evolved through PAD and passive liveness detection to deepfake detection and now IAD. As the market matures, the distinction between these technologies is becoming less important than their combined ability to establish trust in remote digital interactions.

This evolution helps explain why IAD adoption is accelerating across multiple markets simultaneously even though relatively few organizations will issue a dedicated procurement for injection attack detection alone. It provides important context for understanding the next stage of market development: the emergence of integrated identity integrity platforms.

IAD Standards and Testing

Standards are becoming increasingly important as enterprises and government agencies seek independent assurance that vendor claims can withstand real-world attack scenarios.

Biometric IAD is too new as a field of study and set of technologies to have a fully developed regime of standards and testing. This situation, and the wait for the normal process for the development of technical standards to unfold, has contributed to an environment in which biometric PAD is sometimes presented as defense against injection attacks. While PAD can contribute to IAD, however, the new and nascent technical standards reflect the consensus across industries that in real-world fraud scenarios, PAD alone does not constitute comprehensive or robust protection against injection attacks.

Standards specific to IAD do exist, however, and testing programs based on them are now available.

CEN/TS 18099

The European Committee for Standardization (CEN) developed the CEN/TS 18099:2024 specification for "Biometric Data Injection Attacks" and published it in November of 2024.

CEN/TS 18099 defines the attacks and their fraud use case, defines injection attack instruments for bypass attacks in one or more biometric modalities, and IAD systems. It describes risk mitigation for injection attacks, and IAD evaluation procedures.

The standard recognizes "substantial" and "high" levels of protection against injection attacks. High-level protection is among the requirements for the Extended Level of Identity Proofing (LoIP), which in turn is a requirement for EU Digital Identity (EUDI) Wallets with full function to qualify as Qualified Trust Service Providers (QTSPs) under eIDAS 2.0.

ISO/IEC 25456

An international standard for IAD is currently in development, having been published as a working draft in February 2025.

The standard, titled "Information technology — Biometrics — Biometric data injection attack detection," was approved as a committee draft following the close of the comment period for the working draft last year.

The ISO/IEC standard uses CEN/TS 18099 as a breeder document, and the working draft which was approved for the committee draft stage is similar in many key respects to the European standard.

ISO/IEC 25456 provides similar definitions and overviews for biometric injection attacks, their use case in user enrollment and verification, and injection attack instruments. It offers guidance on detection and appropriate risk mitigation, and the creation of a test plan for evaluating IAD systems.

FIDO Alliance Face Verification

The FIDO Alliance operates a Face Verification Certification program and a Biometric Component Certification (BCC) program, each of which include facial liveness and injection attack protection among its criteria

Injection attacks have evolved from niche research concerns into operational fraud threats across industry verticals, and standards bodies, testing laboratories and biometric vendors are now racing to define how resilient identity systems should be evaluated in real-world environments. Certifications, benchmark testing and interoperability frameworks are increasingly critical market differentiators as organizations seek measurable assurance that biometric systems can withstand AI-driven attacks, virtual cameras and manipulated media streams at scale.

Testing Bodies and Accreditation

IAD is an emerging area of testing for accredited biometrics and cybersecurity laboratories.

Because the ISO/IEC standard is still in the early stages of development, testing at this point is mainly carried out in accordance with the CEN/TS 18099 standard.

The National Voluntary Laboratory Accreditation Program (NVLAP) from the U.S. National Institute of Standards and Technology (NIST) provides third-party accreditation to biometrics laboratories for testing based on international standards. Crucially, because the NVLAP program applies to ISO standards, IAD evaluations are not yet within the scope of NVLAP accreditation.

With the qualification, developers, vendors and relying parties should consider labs that are accredited either to the ISO/IEC 17025 standard for "testing and calibration laboratories" by a national standards accreditation body or to the NVLAP program as reliable testing partners.

The FIDO Alliance also sets its own online authentication criteria for biometric systems, and accredits laboratories to evaluate the conformance of systems to that standard.

Independent IAD testing laboratories

There are only a handful of accredited biometrics testing laboratories that have performed IAD evaluations based on the European standard. There are several more that have performed evaluations to the FIDO standard which includes IAD requirements, but does not specifically assess the performance of IAD systems.

Ingenium began carrying out testing in accordance with CEN/TS 18099 in 2025, carrying out evaluations to Level 2 (CEN High), and is also accredited for FIDO Face Verification certifications. The company offers five different levels of IAD evaluations ranging from 25-day tests to CEN Substantial to 50-day tests which Ingenium says exceed the European standard's requirements.

CLR Labs is accredited by COFRAC for ISO 17025-compliant evaluations based on CEN/TS 18099, as well as biometric PAD and performance standards. Because COFRAC is France's national standards body, CLR Labs' accreditation is recognized across the European Union.

The Age Check Certification Scheme (ACCS) entered the IAD market in 2025, launching a CEN/TS 18099-based compliance testing and certification program. ACCS positions the scheme as a mechanism for evaluating resilience against deepfakes, virtual cameras, manipulated signals and injected biometric media. The initiative expands the number of organizations offering independent IAD conformity assessments and reflects growing demand for standardized assurance against software-based biometric attacks. ACCS is accredited by UKAS as a conformity assessment body, rather than to ISO/IEC 17025 as a testing lab.

BixeLab is an NVLAP-accredited lab, and is also accredited by FIDO to certify Face Verification systems. It offers IAD evaluations as a Level 5 test.

The testing ecosystem is also broadening geographically. In addition to specialist biometric laboratories such as Ingenium, ACCS and CLR Labs, FIDO-accredited laboratories including TTA in South Korea, TÜVIT in Germany, Fime, BixeLab and iBeta now support biometric evaluation and certification programs spanning face verification, document authenticity and biometric component testing. The expansion of accredited testing capacity reflects growing demand for independent validation as organizations seek measurable assurance against increasingly sophisticated biometric fraud attacks.

The IAD assurance ecosystem extends beyond standards bodies and vendors to include accredited testing laboratories, conformity assessment organizations and certification programs. As injection attacks become a mainstream fraud vector, independent evaluation is increasingly viewed as a prerequisite for procurement, regulatory compliance and trust. The growing number of laboratories capable of supporting biometric testing and certification reflects the market's transition from emerging technology category to established security discipline.

Biometric Testing, Certification and Standards Ecosystem

Organization	Role	Relevant Standards / Programs
CEN	Standards body	CEN/TS 18099 (Injection Attack Detection)
ISO/IEC JTC 1 SC37	Standards body	ISO/IEC IAD and biometric standards development
FIDO Alliance	Certification program owner	Face Verification Certification, Biometric Component Certification
Ingenium Biometrics	Independent testing laboratory	CEN/TS 18099, IAD certification testing, FIDO Face Verification, PAD and biometric testing
CLR Labs	Independent testing laboratory	CEN/TS 18099, IAD certification testing, PAD and biometric testing
ACCS	Conformity assessment and certification body	CEN/TS 18099-based IAD certification, Extended LoIP assessments
BixeLab	Independent testing laboratory	CEN/TS 18099, IAD certification testing, FIDO Face Verification, FIDO Biometric Component, PAD and biometric testing, Level 5 IAD
iBeta	Independent testing laboratory	CEN/TS 18099, IAD certification testing, FIDO Face Verification, PAD and biometric testing
Fime	Independent testing laboratory	FIDO Face Verification, FIDO Biometric Component, PAD and biometric testing
TTA (Korea)	Independent testing laboratory	FIDO Face Verification, FIDO Biometric Component, Document Authenticity testing
TÜVIT (Germany)	Independent testing laboratory and security evaluation body	FIDO biometric testing, security evaluations
NVLAP	Accreditation body	Accreditation of biometric testing laboratories under ISO/IEC 17025 and ISO/IEC 19795
COFRAC	Accreditation body	Accreditation of biometric testing laboratories under ISO/IEC 17025 and ISO/IEC 19795
UKAS	Accreditation body	Accreditation of biometric testing laboratories under ISO/IEC 17025 and ISO/IEC 19795

iBeta

iBeta.com
Evan Call / Ecall@iBeta.com / 303-513-7189
2675 S Abilene Street, Suite 300, Aurora, CO 80014

iBeta Quality Assurance is one of the most accomplished biometrics test labs in the world, with accreditations overseen by both governmental and private entities. Since 1999, the lab has been providing excellent software quality assurance services to companies of all sizes, across sectors including identity, technology, telecommunications and more. In the biometrics space, it has completed projects for providers including Yoti, Shufti Pro, Incode Technologies, Regula Forensics, and many more, as well as servicing some of the largest names in the global tech space.

After receiving NIST accreditation to ISO 17025, iBeta Quality Assurance quickly became the first lab to receive accreditation to test compliance to the 30107-3 PAD ISO/IEC standard, allowing it to conduct PAD testing to Level 1, then Level 2 – and, most recently, Level 3. It also has accreditations for the FIDO Biometric Certification, Mastercard Biometric Certification, Android Biometric Certification, ISO 19795-10 and ISO 19795-2 biometric performance testing, DEA EPCS Biometric Subsystem Certification.

The company recently launched an injection attack detection (IAD) testing solution against the European standard CENS/TS 18099: 2025, across multiple platforms. It presages the planned 2027 publication of the ISO/IEC standard dedicated to injection attack testing; iBeta will release a IAD testing solution for the ISO standard when it is released.

For injection attack detection evaluation, iBeta first performs a readiness review effort when the test design will be created. This also includes an analysis of the Target of Evaluation (TOE) and preparing the Injection Attack Instruments (IAIs) and Injection Attack Methods (IAMs). Then iBeta will perform testing to Level 2 or Level 3.

Level 2 is expected to take 25 business days and is considered the Substantial test process. Examples include virtual webcam or emulator injections, which plug a camera feed into the system through an emulator. Level 3 testing, which includes a minimum of 30 days for testing and is considered High level testing; covered attacks include systemless rooting of Android devices and kernel manipulation.

Vendors will receive a detailed report describing the test effort.

Ingenium

ingeniumbiometrics.com

Ingenium is an independent ISO/IEC 17025-accredited biometric testing laboratory specialising in identity verification, age estimation, AI and deepfake prevention technologies. Based in Canterbury, UK, the company operates at the intersection of technology, regulation and trust, providing objective, expert evidence of how identity systems perform against the latest known attack methods. Its leadership team brings decades of experience across government security and industry, supported by global partnerships with technology providers, governments, regulators and standards bodies.

Ingenium is accredited to ISO/IEC 17025 as a certified testing laboratory for performance, equity and security testing, including presentation attack detection (PAD) and injection attack detection (IAD), across biometric and document authentication applications. The laboratory's work aligns with internationally recognised standards including ISO/IEC 19795 for biometric performance testing and reporting, ISO/IEC 30107 for biometric presentation attack detection, and CEN TS 18099:2025 for injection attack testing in line with CEN and ETSI requirements.

Ingenium also holds FIDO accreditation as an authorised test laboratory for biometrics and remote identity verification certification programmes, as well as MOSIP accreditation as a trusted testing partner for open-source identity systems. In the UK, the company supports the National Protective Security Authority (NPSA) and wider critical national infrastructure initiatives.

Alongside biometric performance, PAD and document authentication testing, Ingenium has developed advanced capabilities in injection attack detection testing. Its standards-based methodology builds on the approaches defined within CEN TS 18099 and extends beyond basic camera injection techniques to assess vulnerabilities across all stages of biometric and identity document processing. This includes evaluating attack vectors wherever biometric or document data may be intercepted, manipulated or injected.

To remain current with emerging threats, Ingenium continuously researches evolving injection attack techniques, tools and payloads in collaboration with partners across government, academia and industry.

As an independent testing laboratory, Ingenium believes it plays a critical role in establishing robust, evidence-based evaluations of a system's ability to detect and resist sophisticated attacks. Its objective is to produce testing evidence that stands up to scrutiny from buyers, regulators and relying parties alike.

Why Financial Services Firms Need Independent Biometric Security Testing

Ingenium has recently focused on the financial services sector, testing and evaluating remote identity verification applications for organisations across the UK, EU and global markets. This work spans a range of use cases including customer onboarding, authentication, account recovery and account takeover prevention, while also examining the emerging role of digital identity ecosystems and digital wallets within financial services.

The company has delivered both testing and advisory services across consumer, employee and business-to-business identity use cases, helping organisations understand the resilience of their identity systems against evolving attack methods.

Ingenium employs a broad range of attack techniques designed to expose weaknesses within applications, infrastructure and network communications. Its testing extends well beyond camera injection attacks, targeting vulnerabilities throughout the identity verification workflow to replicate the tactics and behaviours used by real-world attackers.

This approach enables highly realistic assessments of injection attack detection functionality within the risk environments faced by financial institutions. Ingenium's IAD testing incorporates robust methods such as function hooking, library exploits and network-based attacks to inject deepfakes, replay attacks and animated imagery into identity verification systems. All testing follows the principles of CEN TS 18099, while extending beyond baseline conformance requirements to evaluate sophisticated attack scenarios.

Ingenium's testing and research programmes are underpinned by a detailed understanding of the threat landscape facing financial services organisations. By adopting an adaptive approach that mirrors real-world attacker methodologies, the company ensures evaluations are not theoretical compliance exercises, but meaningful assessments of security resilience that financial institutions, regulators and customers can trust.

Advancing the State of the Art

Injection attacks have moved from theoretical threat to operational fraud vectors, prompting vendors, testing laboratories and standards bodies to accelerate their efforts to validate real-world resilience against synthetic video and audio attacks, virtual cameras and injected media streams.

Early certifications and independent evaluations are rapidly becoming competitive differentiators as enterprises and governments seek measurable assurance against AI-driven biometric fraud.

iProov is on record warning about the rise in biometric injection attacks as early as 2020, long before injection attacks became widely recognized across the biometrics industry. The company was the first to complete FIDO Face Verification certification, in May, 2024, and successfully completed an evaluation to CEN/TS 18099 Level 2 (High) by Ingenium in November, 2025.

Unissey was the first IAD vendor to be certified against the CEN/TS 18099 standard, in testing conducted by CLR Labs in late-2024. The company then completed certification to CEN/TS 18099 Level 2 (High) by CLR Labs in October, 2025, following IAD certification to the "Substantial" classification months earlier.

Keyless was certified to the "High" level of IAD under CEN/TS 18099 by CLR Labs in August, 2025, making it the first to reach that classification.

FaceTec completed a Level 4 spoof defense evaluation by Praetorian Security in September 2025, one of the first assessments of its kind focused on bypass attacks, data manipulation and data security protections.
The company was also confirmed compliant with CEN/TS 18099 Level 2 (High) in an evaluation by Ingenium in December, 2025.

BioID researchers warned the biometrics community of the need for distinct software to detect synthetic media and the use of injection attacks to deliver deepfakes in 2022. The company added deepfake detection technology to its liveness detection software in 2023.

The pace of certifications and testing activity reflects how rapidly IAD is evolving from an emerging research area into a baseline security requirement for remote biometric identity systems.

Taken together, these certifications, evaluations and product developments suggest the market is moving beyond awareness toward measurable assurance. As injection attacks become a routine component of identity fraud, organizations are increasingly looking for independently validated protection rather than relying solely on vendor claims.

IAD Market Analysis and Forecasts

This section covers market analysis and forecasts for Injection Attack Detection (IAD).

It investigates key drivers, adoption, key applications and sectors for IAD.

From a product perspective, IAD is generally embedded into other biometric identity anti-fraud services, most notably liveness detection, presentation attack detection (PAD) and deepfake detection. It is becoming a crucial part of biometric identity fraud detection and prevention to counteract the growing threat of injection attacks. As such, this report will not forecast for revenue, as IAD is bundled into core liveness and PAD capabilities.

There are three-year forecasts, 2026-2028, covering:

1. Injection Attacks (number of injection attack attempts)
2. IAD checks (number of checks for injection attacks)

IAD Market Analysis

This section investigates key drivers for adoption, important sectors, and applications for the adoption of Injection Attack Detection (IAD).

The four key market drivers for IAD are:

1. Fraud Prevention
2. Evolution from Presentation Attacks to Injection attacks
3. Enabling Remote Identity Verification (eKYC) & Authentication
4. Ensuring compliance with potential regulation

Key Drivers

Fraud Prevention

The rapid rise of generative AI allows fraudsters to create highly realistic deepfake videos and voice clones, which can be injected directly into systems to bypass basic fraud checks.

Remote Identity Verification (eKYC) & Authentication

As more critical digital services move to remote, app-based onboarding (Know Your Customer) and biometric authentication, the risk of virtual camera exploits, emulator usage, and session tampering has increased, requiring robust digital defense mechanisms. Attacks on biometric authentication systems are on the rise as part of the wider account.

Evolution from Presentation Attacks to Injection attacks

Attackers are shifting from physical presentation attacks to injection attacks, which bypass the camera or sensor entirely to inject digital data directly into the application. The increase in injection attacks is related to the ability to scale the attack.

Ensuring Compliance with Potential Regulation

Regulatory requirements, such as PSD2 in the EU and FFIEC in the U.S., along with standards like ISO/IEC 30107-3, now mandate advanced fraud prevention to protect against increasing digital security threats. The EU AI Act includes provisions for identifying and labelling AI-generated content, including deepfakes.

Key Sectors

As IAD is a key component of biometric-driven identity verification, authentication, and assurance, then the key sectors that are adopting the technology are predominantly those that are high-assurance sectors, often highly regulated.

These seven key sectors are leading the way with adoption of IAD detection:

1. Financial Services
2. Government
3. Enterprise
4. Gaming/Gambling
5. eCommerce/Retail
6. Healthcare
7. Travel (includes border control)

Financial Services

AML/KYC regulation is an important driver for the use of IAD in financial services.

Identity related fraud is a growing concern for the financial services sector, driven by AI-Driven fraud attacks on biometric systems. This includes all types of financial fraud including new account opening fraud where criminals use injection attacks to insert fraudulent biometric data, including synthetic and manipulated images, between the point of capture and the biometric processing engine. This includes the insertion of synthetic identity data, injecting a synthetic face during online account opening (KYC) to pass selfie checks.

Injection attacks are also increasingly being used in ATO attacks to fool authentication processes into believing that they are dealing with a genuine financial services customer.

The Crypto industry is one that is frequently attacked with the highest identity fraud rates in financial services. According to Entrust in their 2026 Identity Fraud Report, Crypto has a 6.6 percent fraud rate, versus 1.5 percent for traditional banks.

As a result of increasing levels of financial fraud, IAD is becoming a critical component to detect and deter identity and financial fraud.

Government

Governments are increasingly rolling out digital services to their citizens across the globe, but this comes with risks.

The need to accurately identify citizens accessing digital government services is a vital part of delivering secure digital government services with the need to know that it is a real person accessing them becoming increasingly important.

There are also the risks associated with AI-generated content that purports to be from legitimate politicians which is a serious threat to the rule of law and democracy.

In May 2025, the FBI issued a warning to the public after investigating a malicious campaign targeting former senior US federal or state government officials with deepfakes. The campaign uses AI-generated voice messages impersonating senior US officials.

This is especially important for tax and welfare services and when applying for or renewing government-issued identity documents including Driver's Licenses, National ID, and Passports.

Enterprise

The ability to prove identity is now an integral part of a modern digital workplace supporting a range of enterprise applications including:

1. Onboarding employees: especially important for remote working scenarios.

2. Privileged access control: linked to privileged identity and access management PIM/ PAM).

3. Fraud detection in web conferences: detecting IAD attacks in business web calls.

4. Remote worker authentication: reducing home and remote working fraud where an imposter or alternative worker attempts to gain access to business digital services.

There have been examples of injection attacks on employers. In April 2025, a news story ran that detailed the risks of not doing adequate identity verification for new hires. It was discovered that North Korean IT workers are using deepfake technology to create synthetic identities for online job interviews aimed at securing remote work.

With the easy availability of generative AI and injection attack tools, organizations must ensure that they employ robust and secure technology that can detect and prevent these kinds of AI-driven fraud attacks.

Gaming/Gambling

To counteract fraud and to support proof of age (age assurance) requirements, the gaming and gambling communities are beginning to adopt IAD measures as part of the biometric identity security solutions.

To support secure onboarding and to reduce money laundering liabilities, the ability to prove identity and appropriate age is an important countermeasure to fraud in a sector that has historical problems with organized crime.

eCommerce/Retail

Popular applications where IAD are beneficial include digital onboarding, payment security, and used in combination with face age assurance (estimation).

Governments are increasingly using legislation to prevent young people from accessing restricted goods and services, including alcohol, medication, and dangerous weapons including knives and drugs. Deepfakes are being used in an attempt to get around these checks and can be delivered through injection attacks.

Healthcare

Healthcare providers around the world lose billions of dollars in fraud. The UK's NHS lost £7.5 billion (roughly US$9.3 billion) to fraud in the six-years to 2023.

The FBI lists the following fraud types in relation to common types of health care fraud that are identity related.

1. **Identity theft / identity swapping:** Using another person's health insurance or allowing another person to use your insurance
2. **Impersonating a health care professional:** Providing or billing for health services or equipment without a license.

Combining identity proofing and verification with face liveness, deepfake detection and IAD can be a crucial tool in preventing healthcare fraud.

Travel

The travel industry is a beacon of light for the adoption of portable digital identity, backed by global standards and using government-grade security.

Remote digital services are transforming the travel industry enabling passengers to book tickets, prove their identity with government-issued documents, including passports, check-in to flights, all from the comfort of their home or office – before they leave to travel.

The prevention of injection attacks is becoming a critical consideration for the travel industry in the fight against identity fraud.

Key Applications

Goode Intelligence has identified four key applications that IAD is being used in. The four are:

1. Digital Onboarding

2. Biometric Authentication

3. Financial Transaction Security

4. Identity Verification

Digital Onboarding

Digital onboarding is the process of using technology to integrate new customers or employees into a service or organization. It is often called identity proofing or identity verification.

Biometrics is a vital tool for remote customer onboarding for a wide range of sectors with particularly high adoption in financial services.

IAD is becoming a core component for digital onboarding that prevents spoof attacks, ensuring that the legitimate user is presenting themselves to a device's camera and not via emulation or other injection method.

Identity verification and identity proofing are closely related but serve different purposes in the process of confirming someone's identity.

Identity proofing is the initial step where the goal is to **validate** that a person is who they claim to be. This involves collecting and analysing personal data and documents. It includes gathering information such as name, date of birth, and address, and verifying identity documents like passports or driving licenses. Often, biometric data (like fingerprints or facial recognition) is also used. The result of identity proofing is a validated identity that can be used for further verification steps.

Identity verification is the subsequent step that **confirms** the authenticity of the information and documents provided during the identity proofing stage. It can involve checking the validity of the documents and data collected. Methods can include comparing photographs on identity documents, validating biometric data, or verifying addresses and phone numbers.

Adoption of biometric onboarding services has been strong, driven by a combination of AML/KYC compliance, fraud reduction and digital transformation programs across sectors pushing onboarding to the home through remote, unattended, means.

Biometric Authentication

Biometric authentication is a security process that uses an individual's unique physical or behavioral characteristics to verify their identity, comparing the presented biometrics to a stored version (template). Biometrics are increasingly being used for authentication, especially in multi-factor authentication scenarios.

Widely deployed modalities for biometric authentication include face, fingerprint, and voice – all modalities that can be spoofed through injection attacks.

IAD enhances face biometric authentication by ensuring that the presented face is a real, authorized person, especially when combined with other biometric fraud protection tools including presentation attack and deepfake detection.

According to recent research, attacks on authentication systems, as part of Account Takeover (ATO) attacks, are increasing. The UK's fraud network, CIFAS, recorded more than 242,000 cases of identity fraud in 2025, with fraudsters increasingly targeting account takeovers, particularly via mobile phones. The Smile ID 2026 Digital Identity Fraud in Africa Report discovered that ATOs were dominating fraud in the region with the movement of fraud attacks from account opening (onboarding) to login (authentication) and transacting.

Financial Transaction Security

There have been several accounts of financial fraud where large sums of money have been transferred to fraudsters believing they are dealing with legitimate colleagues, clients, or partners.

In 2024, a report from Hong Kong Police said that a finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call. The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact AI recreations.

The ability to detect injection and deepfake attacks are now important considerations for financial transaction security.

Identity Verification

Identity verification (IDV) establishes that a person is who they claim to be. It's used in a variety of situations including digital onboarding, for instance opening a bank account, proving how old we are (age assurance), traveling (especially when traveling across international borders), applying for, and starting, a job (employment onboarding), joining an educational establishment, including college and university, buying a new mobile phone, buying a new home.

IAD is now an integral part of the identity verification processes, helping to ensure that the identity being verified is authentic and vendors are increasingly offering IAD solutions as part of the biometric fraud detection suite of products.

IAD Forecasts

Introduction

Market forecasting is very important in the Goode Intelligence (GI) research and analysis methodology especially when dealing with new or emerging markets and products.

GI has an excellent track record of forecasting in emerging technology areas including correctly predicting the growth of the mobile as an authentication device in 2009, the emergence of biometrics on mobile devices in 2011, and the growth in digital identity in 2015.

Market forecasting is one of the tools that GI uses in predicting the degree of success a new product or service will enjoy in the marketplace. The GI methodology considers areas such as product awareness, distribution, price, fulfilling unmet needs and competitive alternatives.

GI creates forecasts by gathering data from diverse sources like company filings, economic reports, and direct interactions (interviews) with both suppliers and buyers, some of which are bound by NDAs. GI then applies both quantitative methods and qualitative assessments (such as expert opinions) within financial models. These models are designed to estimate future performance by incorporating macroeconomic factors, industry trends, and company-specific details to provide a comprehensive view of expected growth and profitability

We always welcome feedback from readers on the accuracy of the forecasts and are open to reflecting your opinion in future reports.

There are three-year forecasts, 2026-2028, covering:

1. Injection Attacks (number of injection attack attempts)
2. IAD checks (number of checks for injection attacks)

The forecasts on total number of injection attacks have been formulated through a combination of interviews (mostly under NDA) and through current identity fraud reports, most notably:

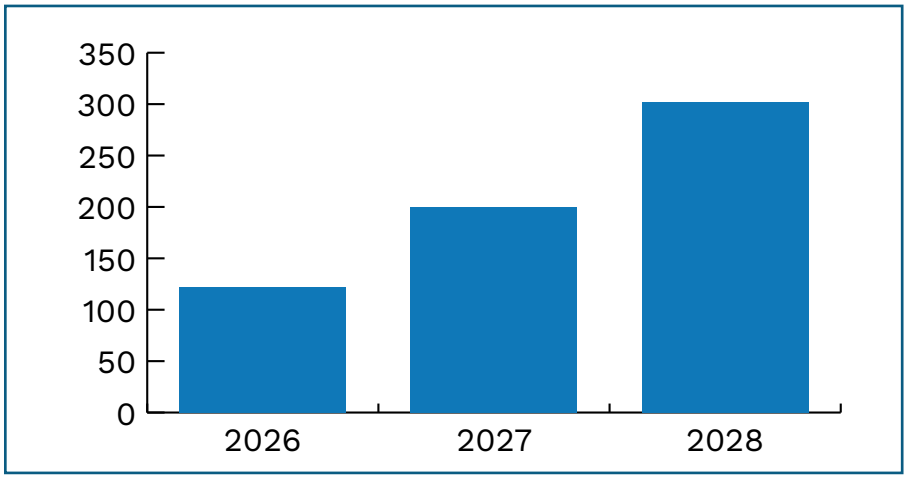
- Entrust Identity Fraud Report 2026
- Smile ID 2026 Digital Identity Fraud in Africa Report
- Cifas 2026 fraud landscape

From a product perspective, IAD is generally embedded into other biometric identity anti-fraud services, most notably liveness detection, presentation attack detection (PAD), and deepfake detection. It is becoming a crucial part of biometric identity fraud detection and prevention to counteract the growing threat of injection attacks. As such, this report will not forecast for revenue as IAD is bundled into core liveness and PAD capabilities.

IAD Forecasts – Total global injection attack attempts

These forecasts are for the total number of injection attack attempts made annually.

Chart 1: IAD Forecasts: Total Global Injection Attacks (m)



Source: Goode Intelligence © 2026

Table 1: IAD Forecasts: Total Global Injection Attacks (m)

	2026	2027	2028
Total	122.32	199.86	301.73

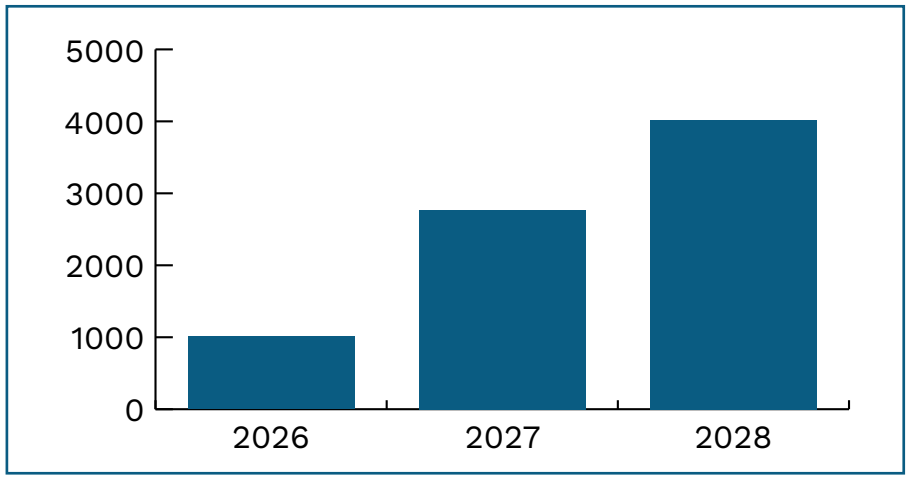
Source: Goode Intelligence © 2026

Injection Attacks will exceed 301 million annually by 2028

IAD Forecasts – Checks

These forecasts are for total global injection attack detections made annually.

Chart 2: IAD Forecasts: Total Global Checks (m)



Source: Goode Intelligence © 2026

Table 2: IAD Forecasts: Total Global Checks (m)

	2026	2027	2028
Total	1014.09	2765.34	4021.21

Source: Goode Intelligence © 2026

Injection Attack Detection Checks will exceed 4 billion annually by 2028

Injection Attack Detection Buyers Guide

This section provides potential buyers of Injection Attack Detection (IAD) products and services with a guide to how to assess solutions.

It is important to note that this guide should not be used as the sole method for assessing IAD solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

The buyers guide also includes a list of IAD vendors (suppliers) that are active in the market. For a select number of vendors, there is a profile of the company and their products.

Biometric Update and Goode Intelligence strives to provide accurate information, but we must point out that our list of vendors is not comprehensive. We have selected a representative group of vendors, but we do not guarantee that our list is exhaustive. The analysis is presented on a "best efforts" basis, and we cannot accept any liability for any errors or omissions.

If a vendor considers that we have unreasonably omitted them then there is an opportunity for them to engage with Biometric Update and Goode Intelligence for inclusion in subsequent editions of this report.

What to look for in an IAD supplier

This section provides a guide for buyers in what to look for in an IAD supplier.

It is important to repeat that this guide should not be used as the sole method for assessing IAD solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

IAD solutions are predominantly sold as part of liveness detection and deepfake detection solutions, as part of anti-fraud measures in biometric identity and authentication systems to answer these critical questions when a person is onboarding or authenticating; is the person present, genuine, alive, and not a spoof or synthetically generated.

When choosing a biometric IAD supplier, buyers must move beyond traditional presentation attack detection to address sophisticated digital threats like synthetic identities, virtual cameras, and emulator attacks. A robust supplier should offer defense-in-depth, combining AI-driven detection with secure system architecture.

Baseline criteria

This report identifies the following baseline criteria for measuring whether an IAD solution is suitable.

1 **Cost - does it meet your budget expectations:** This is especially important when dealing with suppliers that charge per transaction, which is often the case. If you are entering into a per transaction contract, have you sized your requirements for now and for future growth and does your budget meet this? Is there a separate fee for IAD checks, or is it part of liveness and presentation attack detection solutions?

2 **Advanced threat coverage:** Injection attacks bypass the physical camera by inserting data directly into the system stream (e.g., using virtual cameras, emulators, or API hooks).

1. **Virtual Camera and Emulator Detection:** Can the supplier detect if a video feed is coming from an emulator or a virtual webcam rather than a real device camera?
2. **Deepfake and Synthetic Media Detection:** Does the solution use specialized AI algorithms to detect manipulated video (deepfakes) or computer-generated faces?
3. **Stream Integrity Checks:** Can they analyze the video feed for anomalies, such as frame inconsistencies, unusual resolutions, or mismatching device metadata?
4. **API Hooking Mitigation:** Does the vendor provide tools to detect if the biometric application's code is being tampered with at runtime?

3 **Certification and Proven Performance:** Does the solution adhere to IAD standards including CEN/TS 18099:2024 (Biometric Data Injection Attack Detection) and has it been tested/certified against this standard. In addition to CEN/TS 18099:2024, does the solution adhere to ISO/IEC 30107-3 (Presentation Attack Detection) and has been certified to this standard by an established test company.

4 **Accuracy and Speed:** The software should have high accuracy (low false positives and false negatives) and be able to process media quickly.

5 **Security:** Does the supplier have cybersecurity certifications and adhere to cybersecurity guidance / best practice? Can the vendor provide hardened software or mobile SDKs to ensure the camera feed remains secure from the device to the backend? Ensure the supplier has been tested by external, independent, or accredited penetration testing agencies, as injection attacks differ from traditional "spoofing".

6 **Does it meet your specific usability requirements?** The ability to fit in with your usability (UX) requirements is an important consideration when choosing an IAD supplier.

7 **Privacy and data protection compliance:** Does it meet EU GDPR and other state legislation related to the collection, storage and use of biometric data?

8 **Integration:** Check whether the solution can be easily integrated into existing identity management and fraud management systems and workflow.

9 **Scalability:** Can the supplier handle a high volume of transactions without decreasing detection speed or accuracy?

10 **Independent validation:** Has the solution been evaluated by an accredited third-party laboratory? Are evaluation results publicly available?

IAD Vendor Profiles and Case Studies

Biometric Update and Goode Intelligence have identified approximately 30 vendors that offer Injection Attack Detection (IAD) solutions either as a module or standalone option, or as part of a liveness, fraud prevention or all-in-one identity verification suite. This directory presents a representative group of vendors, but our list is not exhaustive. If a vendor considers that we have unreasonably omitted them then there is an opportunity for them to engage with Biometric Update and Goode Intelligence for inclusion in subsequent editions of this report.

Identy.io

identy.io
contact@identy.io

Headquartered in the U.S. with offices in Brazil, Mexico, Colombia, Nigeria, Spain and India, Identy.io delivers universal digital identity at scale, powered by ABIS and reusable digital credentials, while turning any smartphone camera into a multimodal biometric scanner capable of capturing face, fingerprint and palm.

As face biometrics emerges as the primary alternative to passwords for remote identity verification, it is becoming a primary target for industrialised fraud at scale. The first wave of attacks came through physical presentation — photos, screens, masks — and the industry responded with Presentation Attack Detection (PAD). Today, attack kits combining camera injection with AI-powered deepfake generation are increasingly accessible, requiring almost zero expertise. These tools defeat traditional PAD systems entirely by overlaying a target identity onto the attacker's live camera feed, following blinks, smiles and head turns naturally. There are no physical artifacts for passive systems to detect and no active challenges they cannot answer.

Identy.io responded to injection attacks with two independent layers. Injection attack prevention protects the integrity of the capture pipeline — camera, device and code — ensuring the biometric sample was captured from a real physical sensor. Deepfake detection then analyses the biometric material directly, identifying AI-generated or manipulated faces. Defeating one layer does not defeat the other.

Despite these specific countermeasures to address injection attacks, the fact that facial verification is the primary attack target reveals a structural vulnerability: face is the most exposed modality, with billions of images publicly available on social networks. For operations requiring higher security, face alone is not sufficient and additional authentication factors are required. Identy.io enables fingerprint capture using any smartphone camera, creating a multimodal layer that is structurally harder to attack: fingerprint data is far harder to obtain than facial images, with no public corpus.

Current implementations relying on server-side architectures reveal an additional weakness: any device can capture and submit biometric data for comparison against a centrally stored template. Identy.io executes the complete authentication pipeline on the device itself, including matching against the user's registered biometric. Match-on-device requires the attacker to be physically present on the specific device where the registered biometric lives, making large-scale attacks structurally unviable.

Incode

incode.com

Incode is a digital identity platform that secures how humans verify themselves online. With visibility into more than 7.1 billion trust checks, it is used by 8 of the 10 top U.S. banks, and supports organizations across financial services, telecom and government.

The threat of injection attacks has escalated sharply alongside the availability of generative AI tools. Face-swap tools and synthetic face generators that previously required technical expertise are now widely accessible. According to the Deloitte Center for Financial Services, AI-enabled fraud losses grew from $12.3 billion in 2023 and are projected to reach $40 billion by 2027.

Deepsight is Incode's deepfake and injection attack detection product. It uses a three-layer AI system, covering perception, device integrity, and behavioral signals, to detect synthetic and injected media in real time while adding zero friction. The Perception Layer uses a multimodal AI model across video, motion, and depth to catch cross-modal inconsistencies. The Integrity Layer blocks virtual cameras, emulators, and injected media at the device level. And the Behavioral Layer spots fraud farm patterns and automated flows.

The experience is fully passive: the user does not have to move, smile, or take any additional action beyond what standard verification already requires.

Deepsight is purpose-built for identity verification entirely on its proprietary stack, with no third-party detection components. That enables it to fine-tune the model directly against specific attack patterns and fraud signals seen in production across more than 4 billion identity checks per year.

Benchmarked internally against the detection approaches most commonly used across the industry, Deepsight showed 68x better false-positive rate than the next-best commercial solution on identity verification use cases. The model updates continuously, tied to monitoring live attack patterns in production, not just published benchmarks.

The first standard built specifically for injection attack detection is CEN/TS 18099:2025, a European technical specification that defines test methodology and evaluation levels for IAD. Most PAD certifications from iBeta do not cover injection attacks; CEN/TS 18099 evaluations are newer, fewer vendors have completed them, and independent lab capacity is still limited. But Incode monitors and aligns with the evolving standards landscape. As CEN/TS 18099 evaluations become more widely available, independent validation of IAD capabilities will be an important signal for any serious procurement process.

Innovatrics

innovatrics.com
sales@innovatrics.com
Tomášikova 64, 831 04 Bratislava, Slovakia
+421 2 2071 4056

Innovatrics is an independent, EU-based provider of trusted biometric solutions used by governments, businesses, and law enforcement agencies to keep people safe, onboard new customers, and build institutional trust. Headquartered in Bratislava, Slovakia, the company's algorithms have consistently ranked among the fastest and most accurate in fingerprint, face and iris recognition in benchmarks and evaluations.

Innovatrics' solutions are used globally across regulated and high-volume digital services, primarily banks, fintech companies, telecom operators and digital platforms that rely on secure remote onboarding. However, it is seeing rising adoption in non-regulated sectors such as retail, online marketplaces and hospitality. The company prioritizes cooperation with clients and real-world feedback, working closely with institutions across multiple markets and use cases. Regionally, deployment is strongest in Europe, the Middle East, and Latin America, where organizations face increasing AI-driven identity fraud and evolving compliance requirements.

Innovatrics develops all of its core identity verification components internally, including auto-capture, OCR and biometric matching, liveness and injection attack detection. Rather than relying on a single protective mechanism, it secures the full onboarding flow, combining document validation, multiple liveness options, camera feed authentication, and deepfake detection. Owning the full stack allows it to fine-tune deployments to specific regulatory, risk, and user experience requirements.

The company has observed a global rise in injection and deepfake attacks, increasingly overtaking traditional presentation attacks such as printed photos or screen replays. Attackers now combine stolen personal data, generative AI, face morphing and virtual camera tools to bypass remote onboarding at scale. Because the underlying identity data may be real, standard document validation alone is not always sufficient. Exposure varies by business model, with higher risk for organizations that enable immediate financial gain, access to credit, digital assets, telecommunications services or other monetizable benefits.

The company's Injection Attack Detection technology protects remote identity verification from video injection and deepfake attacks, authenticating the camera feed and verifying that the video stream originates from a genuine device camera rather than an emulator, replay, or virtual source. Running during digital onboarding, it adds a robust security layer beyond standard liveness detection. According to company data, after deploying injection attack detection together with deepfake detection, organizations report that most attacks are identified and prevented during onboarding.

Innovatrics is aiming to obtain certification under the biometric data injection attack detection standard CEN/TS 18099:2024 in the second half of 2026.

Mitek

miteksystems.com
770 First Avenue, Suite 425, San Diego, CA 9210
619.269.6800

San Diego, California-based Mitek helps businesses verify identities, prevent fraud and deliver secure, seamless digital experiences in the face of rapidly advancing AI-generated threats. From deposits to identity verification and authentication, Mitek's technology safeguards critical digital interactions: more than 7,000 organizations rely on Mitek to protect their most important customer connections.

Injection attacks are an emerging fraud technique targeting digital identity verification systems. Awareness of injection attacks is increasing, but many organizations are still early in understanding the scale of the risk. Mitek's analysis of fraud attempts across large financial institutions in 2025 shows how quickly this threat is evolving. While deepfake-driven fraud initially occurred more frequently, injection attempts grew rapidly throughout the year, reaching nearly 200 percent relative to deepfake incidents by year end.

Adoption of injection attack detection is strongest in sectors that rely heavily on remote identity verification and operate in environments where fraud risk is high. Financial institutions and fintech companies are among the earliest adopters, particularly for digital account onboarding, payments, authentication, and account recovery workflows where identity assurance is critical.

Mitek detects injection attacks targeting identity verification and biometric systems. Using AI-driven analysis, the technology monitors digital content and transmission channels for artifacts of injected media, identifying deepfakes and other manipulated content inserted into the capture stream and preventing fraudulent inputs from reaching verification workflows. Its technology has been pressure-tested in high-risk environments, including deployments with many of the world's largest financial institutions.

The solution is designed for the reality that modern fraud rarely relies on a single tactic. Attackers increasingly combine techniques such as deepfake manipulation and injection attacks to bypass individual controls. By evaluating multiple fraud signals rather than focusing on a single indicator, organizations can detect sophisticated attacks even as fraudsters shift methods.

It extends protection across the digital identity lifecycle, from onboarding to authentication, account recovery, and other high-risk interactions. Monitoring for injected or manipulated media throughout these digital journeys helps organizations identify threats earlier and reduce exposure.

Across any organization that depends on trusted digital interactions, there is growing focus on defending against account takeover and other digitally engineered attacks. As attackers increasingly target the digital capture pipeline itself, organizations are recognizing the need for detection capabilities designed specifically to identify injected media before it reaches verification systems.

Stopping an AI-Driven Injection Attack During Digital Onboarding

Industry: Banking
Institution: Top U.S. Bank

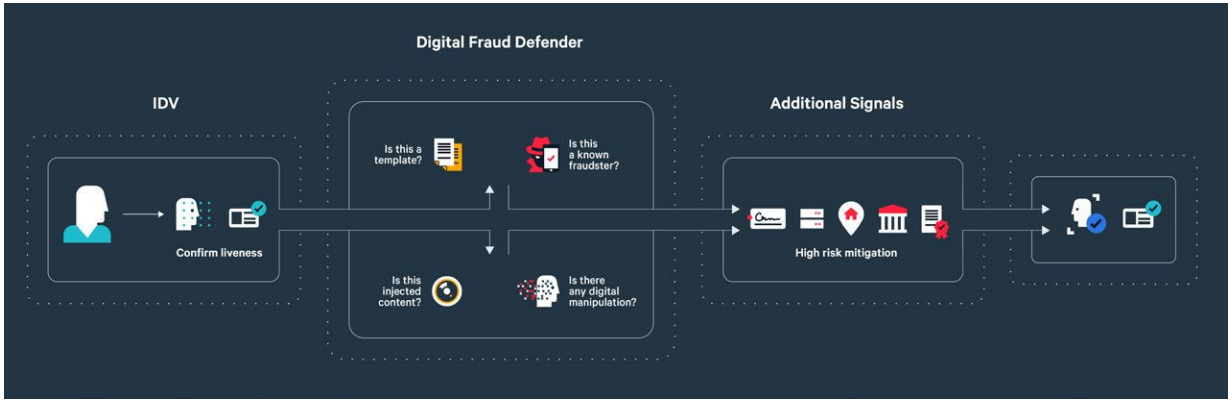
The Challenge

A Top Bank was targeted by an AI-driven injection attack during digital account onboarding. Fraudsters launched more than 600 coordinated attempts using a single device (Google Pixel 4a, "Sunfish"), submitting varied documents and selfies to evade detection.

The bank's existing fraud controls failed to recognize the attack pattern, exposing a critical security gap and creating potential for significant fraud losses.

The Solution

Through the addition of highly tuned injection-attack detection signals, Mitek identified suspicious behavioral patterns and escalated activity for review. By implementing a layered fraud detection strategy, the bank was able to uncover and stop an attack vector that its legacy controls had missed.



The Impact

- **4.3%** of transactions flagged as suspicious
- Injection attack signals were the **sole fraud authenticator in 70%** of flagged cases
- Customer approval rates remained strong (**88.1% → 88.7%**)
- Confirmed fraud cases reported via SAR filings

Business Outcome

The bank prevented fraud losses while maintaining a seamless onboarding experience. The incident reinforced the value of layered, AI-driven fraud protection in defending against sophisticated injection attacks.

OZ Forensics

ozforensics.com
Office 384, Saih Shuaib bldg 2 area,
DIC, Dubai UAE

Oz Forensics is globally recognized for advanced liveness detection and face biometrics solutions. Chosen by financial institutions, telcos and governments to fight deepfakes and digital fraud in more than 20 countries, its technology delivers protection against sophisticated attacks on remote KYC and identity verification. Clients span LATAM, Europe, the Middle East and Central Asia and Southeast Asia, supporting more than 1.5 billion liveness checks per year.

Oz Liveness Injection Attack Detection combines SDK environment integrity checks with neural network analysis of incoming media, to stop injection attacks on biometric capture, including virtual camera feeds, emulator or rooted devices, and network or API tampering. The technology offers full deployment flexibility to meet organizational needs, supporting on-premises, hybrid/private cloud, and SaaS environments, with availability via AWS and Huawei marketplaces. In real-world production environments in 2025, Oz patented technology, including 50+ ML/AI models, a proprietary data container, and mobile/web SDKs, prevented more than 0.5 million fraud attacks, with Injection Attacks alone accounting for over 45 percent of all the fraud attempts.

The solution has been independently evaluated by BixeLab against biometric presentation attacks and injection attack scenarios, using ISO/IEC 30107-3 and CEN/TS 18099, respectively. In the independent evaluation, Oz Forensics achieved an observed APCER of 0 percent for the presentation attack instruments included within the agreed test scope. Of the testing process, Dr. Ted Dunstone, CEO and founder of BixeLab, says "we routinely see that the hardest failures to detect are the ones that look like normal capture. An independent injection attack detection evaluation is about proving the system can detect data-stream substitution attempts without materially increasing false rejects for genuine users."

The ISO/IEC 25456 standard, now under development as a Working Draft, will establish the methodology for evaluating injection attack detection systems and define risk-mitigation measures. Since ISO/IEC 25456 is based on CEN/TS 18099, Oz Forensics' technology already meets its anticipated requirements and is prepared for official certification immediately upon the standard adoption.

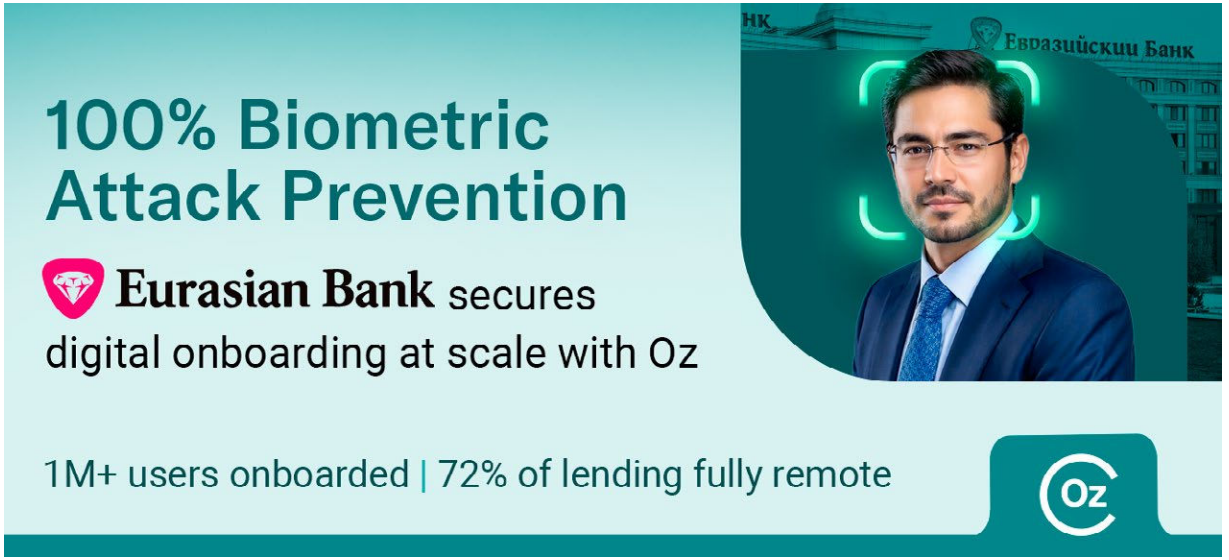
Says Oz Forensics Chief Information Security Officer Artem Tulenov, "official certification serves as the sole instrument for independent and objective security assessment, enabling stakeholders to distinguish marketing claims from the actual resilience of solutions against contemporary threats."

Preventing Biometric Attacks in Digital Banking at Scale

Eurasian Bank, one of Kazakhstan's largest retail financial institutions, launched a digital transformation initiative to move onboarding and lending services to fully remote channels. As digital adoption increased, secure and reliable biometric verification became essential to maintain trust and prevent fraud.

The bank faced growing risks from biometric threats such as deepfakes and other forms of identity fraud, as well as emerging injection-based attacks affecting digital identity systems. To respond to these challenges, Eurasian Bank partnered with Oz Forensics to strengthen its remote verification processes.

The solution combined facial recognition with liveness detection and additional security measures to improve protection against evolving threats. This approach increased the reliability of remote identity checks while keeping the user experience simple and efficient.



The results were clear. Eurasian Bank prevented 100% of biometric attacks in production, showing strong protection against fraud. At the same time, the bank onboarded more than 1 million users through digital channels, accelerating customer acquisition.

Remote biometric identification became a key part of the bank's operations, accounting for 72% of all lending in Q4 2022. This reflects both improved efficiency and growing customer trust in digital services.

This case shows how financial institutions can expand digital services securely while adapting to new types of fraud.

Youverse

youverse.id
sales@youverse.id
Taguspark, Núcleo Central, 147, 2740-122
Oeiras, Lisbon, Portugal

Youverse provides enterprise-grade biometric verification for high-assurance digital identity, combining face biometrics, liveness, age estimation, Presentation and Injection Attack Detection (PAD/IAD) and document verification. Its privacy-first, sharded and distributed biometric architecture prevents template reconstruction, reduces breach risk and supports secure onboarding and authentication.

Youverse is used by government digital identity programs, banks, fintechs, telecom operators, online gaming platforms, age-restricted services, trust service providers and digital identity wallet providers. Its adoption is in Europe, the UK, Latin America and the Middle East, with growing demand from regulated financial services, identity ecosystems and organizations preparing for eIDAS 2.0 requirements.

Injection attacks are becoming a serious threat to remote identity verification because they bypass the camera rather than fool it. Awareness is increasing, but many buyers still underestimate the risk. Youverse Injection Attack Detection protects biometric journeys from camera bypass, replay, emulator, virtual camera, API and deepfake injection attacks. It validates capture integrity, device signals and biometric data provenance in real time, delivered through SDKs and APIs, with pricing aligned to transaction volume, risk level and deployment model.

Using injection protection and liveness from a single biometrics provider enhances security by tightening acquisition and processing components. The liveness engine, capture SDK, integrity checks and server-side IAD controls operate as a unified chain of trust, reducing gaps between separate vendors or disconnected components.

Youverse operates in an evolving standards landscape. ISO/IEC 30107-3 is the established standard for biometric presentation attack detection testing and reporting. Youverse has been successfully tested by iBeta for conformity against ISO/IEC 30107-3 Level 2. For injection attack detection, the key European development is CEN/TS 18099, which addresses biometric data injection attacks and provides a methodology for evaluating resistance. In Europe, ETSI TS 119 461 is becoming central to remote identity proofing under eIDAS 2.0, and for Level High assurance, injection detection evidence according to CEN/TS 18099 is a key compliance requirement by end of 2026.

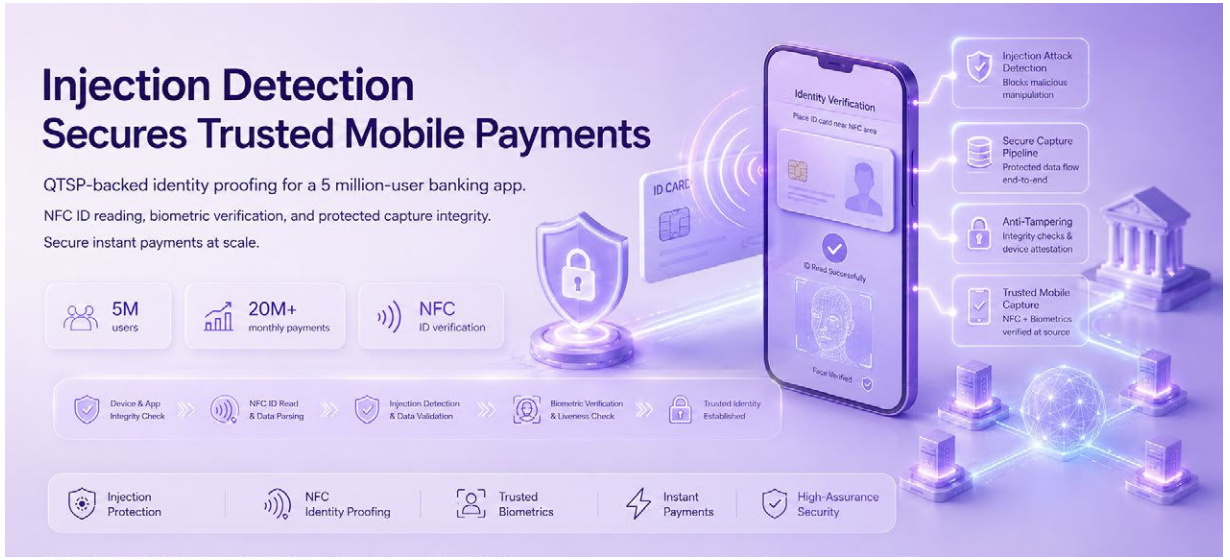
Youverse products are built to support conformance with ISO/IEC 30107-3 and ISO/IEC 19989 and the company is delivering its IAD capabilities according to CEN/TS 18099 and level High of the Extended Level of Identity Proofing requirements associated with ETSI TS 119 461 and eIDAS 2.0.

IAD Secures Five Million Bank Payment App Users Daily

A qualified trust service provider is using Youverse injection attack detection to strengthen remote identity proofing for a 5 million-user mobile payment platform processing more than 20 million transactions each month.

The platform enables bank customers to prove identity on their phone by reading an ID card via NFC and completing biometric verification in the same mobile journey. This creates a high-assurance, low-friction route for users to access instant online payments at scale.

Useful for general user onboarding inline with new extended level of identity proofing required by eIDAS 2.0, the use case is especially relevant under the EU Instant Payments Regulation, Regulation (EU) 2024/886, which makes 10-second, 24/7 instant euro credit transfers the new standard and requires instant payments to cost no more than standard transfers. It also removed the previous €100,000 scheme limit, making strong identity proofing and fraud-resistant authentication even more important as banks support higher-value digital payments.



Youverse protects the flow against camera bypass, virtual camera, emulator, replay and manipulated biometric data attacks. By combining liveness and injection protection from one provider, the QTSP gains tighter control over acquisition and processing, reducing the gaps that can appear when capture integrity, biometric assessment and server-side risk controls are split across vendors.

The result is a trusted mobile identity layer that supports secure, high-volume instant payments and onboarding routes without compromising user experience.

Select IAD Vendors

A

AU10TIX

au10tix.com

AU10TIX is a private identity verification company founded in 2002 and headquartered in Nicosia, Cyprus. The company provides identity verification, document authentication and fraud prevention technologies for financial institutions, marketplaces and regulated industries worldwide.

AU10TIX combines identity verification, biometric checks and fraud intelligence capabilities to help organizations detect synthetic identities, deepfake-enabled fraud and biometric injection attacks during remote onboarding and account creation.

Aware

aware.com

Aware is a publicly traded biometric software company founded in 1986 and headquartered in Burlington, Massachusetts, USA. The company develops biometric authentication and identity verification technologies for government, border management, law enforcement and commercial applications.

Aware offers biometric authentication and liveness detection capabilities designed to help organizations defend against presentation attacks, synthetic identities and biometric injection attacks in remote onboarding and authentication environments.

B

BioID

bioid.com

BioID is a private biometric authentication company founded in 1998 and headquartered in Nuremberg, Germany. The company specializes in biometric identity verification, authentication and liveness detection technologies for financial services, healthcare, government and enterprise applications.

BioID combines facial biometrics, liveness detection and anti-spoofing technologies to help organizations defend against presentation attacks, deepfakes and biometric injection attacks. Its platform is designed to verify that biometric data originates from a genuine user and trusted capture environment during remote onboarding and authentication processes.

D

Daon

daon.com

Daon is a private identity assurance and biometric authentication company founded in 2000 and headquartered in Fairfax, Virginia, USA. The company provides digital identity verification and authentication solutions for banking, healthcare, telecommunications and government sectors.

Daon's identity assurance platform combines biometrics, liveness detection and fraud prevention technologies to help organizations mitigate deepfake-driven fraud, account takeover attempts and biometric injection attacks.

E

Entrust

entrust.com

Entrust is a private security and identity technology company founded in 1969 and headquartered in Minneapolis, Minnesota, USA. The company provides identity verification, credential issuance, PKI, digital signing and biometric authentication technologies.

Entrust offers identity verification and liveness detection capabilities designed to help organizations detect sophisticated injection attacks, AI-generated identities and deepfake-enabled fraud during remote onboarding and authentication.

F

Facephi

facephi.com

Facephi is a publicly traded biometric technology company founded in 2012 and headquartered in Alicante, Spain. The company specializes in digital identity verification, biometric authentication and fraud prevention technologies for financial services and regulated industries.

Facephi combines facial biometrics, liveness detection and behavioral analysis technologies to help organizations defend against spoofing attempts, synthetic identities and biometric injection attacks.

FaceTec

facetec.com

FaceTec is a private biometric software company founded in 2013 and headquartered in Las Vegas, Nevada, USA. The company specializes in 3D face verification and liveness detection technologies used in digital identity and authentication systems.

FaceTec's platform is designed to detect presentation attacks and sophisticated biometric injection attacks, including AI-generated deepfakes and digitally injected video streams used to bypass remote identity verification systems.

G

GBG

gbg.com

GBG is a publicly traded identity intelligence company founded in 1989 and headquartered in Chester, UK. The company provides identity verification, fraud prevention and digital onboarding solutions for financial institutions, governments and regulated industries worldwide.

GBG combines identity verification, biometric authentication and fraud prevention technologies to help organizations address deepfake-enabled fraud, synthetic identities and injection attack threats during remote onboarding and authentication workflows.

I

ID-Pal

id-pal.com

ID-Pal is a private identity verification company founded in 2016 and headquartered in Dublin, Ireland. The company provides AI-powered

identity verification and compliance technologies for financial services and regulated industries.

ID-Pal combines facial biometrics, document verification and liveness detection to help organizations defend against identity fraud, deepfake attacks and biometric injection attempts during customer onboarding.

Idemia

idemia.com

Idemia is a private identity and security technology company founded in 2017 and headquartered in Courbevoie, France. The company provides biometric identification, authentication and identity verification technologies for governments, enterprises and financial institutions worldwide.

Idemia develops advanced biometric security and liveness detection technologies designed to help organizations counter presentation attacks, synthetic identities and increasingly sophisticated biometric injection attacks.

Identy.io

identy.io

Identy.io is a private biometric identity verification company founded in 2014 and headquartered in Dover, Delaware. The company provides mobile-first biometric authentication, identity verification and fraud prevention technologies for financial services, government and enterprise applications.

Identy.io combines facial biometrics, liveness detection and device integrity technologies to help organizations defend against deepfakes, virtual cameras, emulators and biometric injection attacks. Its platform uses on-device processing and camera integrity verification to help ensure biometric data originates from a genuine user and trusted capture environment during remote onboarding and authentication.

Incode

incode.com

Incode is a private digital identity company founded in 2015 and headquartered in San Francisco, California, USA. The company provides AI-driven identity verification and biometric authentication technologies for banking, commerce, hospitality and government applications.

Incode's platform combines facial biometrics, liveness detection and fraud analytics to help organizations detect deepfakes, synthetic identities and biometric injection attacks during onboarding and authentication.

Innovatrics

innovatrics.com

Innovatrics is a private biometric technology company founded in 2004 and headquartered in Bratislava, Slovakia. The company develops biometric identification and authentication systems for government, border control and commercial identity applications.

Innovatrics provides facial biometric verification and liveness detection technologies designed to help organizations prevent spoofing attacks, synthetic identity fraud and biometric injection attacks.

iProov

iproov.com

iProov is a private company founded in 2011 and is headquartered in London, UK. The company specializes in biometric facial verification technology, providing solutions for secure online identity verification and authentication.

iProov offers a layered approach to injection attack and deepfake detection effective against sophisticated attacks.

J

Jumio

jumio.com

Jumio is a private company founded in 2010 and headquartered in Sunnyvale, California, USA. Jumio specializes in digital identity verification and authentication services, utilizing technologies such as artificial intelligence, biometrics, machine learning, and liveness detection.

Its solutions help organizations across various sectors, including financial services, digital currency, retail, travel, and online gaming, to onboard customers quickly, prevent fraud, and comply with regulatory requirements. Jumio validates the user's ID, corroborates it with a selfie and uses advanced liveness detection to ensure the person is actually present, not a deepfake.

K

Keyless

keyless.io

Keyless is a private biometric authentication company founded in 2019 and headquartered in London, UK. The company provides privacy-preserving biometric authentication and identity verification technologies for financial institutions, enterprises and digital service providers.

Keyless combines facial biometrics, liveness detection and anti-injection technologies to help organizations defend against deepfakes, virtual cameras, emulators and biometric injection attacks. Its platform is designed to verify that biometric data originates from a genuine user and trusted device, supporting secure remote onboarding and authentication in high-assurance identity environments.

M

Microblink

microblink.com

Microblink is a private identity verification and computer vision company founded in 2013 and headquartered in New York. The company develops document verification, biometric authentication and digital identity technologies for financial services, travel and online commerce.

Microblink combines document verification, facial biometrics and liveness detection capabilities to help organizations identify spoofing attempts, synthetic identities and biometric injection attacks in digital onboarding workflows.

Mitek

miteksystems.com

Mitek is a publicly traded digital identity and fraud prevention company founded in 1986 and headquartered in San Diego, California, USA. The company provides mobile identity verification, biometric authentication and fraud detection technologies.

Mitek combines document verification, facial biometrics and liveness detection technologies to help organizations identify deepfakes, synthetic identities and biometric injection attacks in digital onboarding environments.

Mobbeel

mobbeel.com

Mobbeel is a private biometric identity verification company founded in 2009 and headquartered in Cáceres, Spain. The company provides biometric authentication, identity verification and digital onboarding technologies for financial institutions, government agencies and regulated industries.

Mobbeel combines facial biometrics, liveness detection and fraud prevention technologies to help organizations defend against deepfakes, synthetic identities and biometric injection attacks. Its platform is designed to support secure remote onboarding and authentication by verifying the integrity of biometric capture and helping ensure that identity data originates from a genuine user.

O

Ondato

ondato.com

Ondato is a private identity verification and compliance technology company founded in 2018 and headquartered in Vilnius, Lithuania. The company provides identity verification, KYC, AML and customer onboarding solutions for financial institutions, fintechs and other regulated organization.

Ondato combines document verification, facial biometrics, liveness detection and fraud prevention technologies to help organizations defend against deepfakes, synthetic identities and biometric injection attacks. Its platform is designed to support secure remote onboarding and identity verification by helping ensure that biometric and identity data originate from a genuine user and trusted capture environment.

Oz Forensics

ozforensics.com

Oz Forensics is a private cybersecurity and biometric fraud prevention company headquartered in Cyprus. The company specializes in AI-powered deepfake detection and digital identity fraud prevention technologies.

Oz Forensics develops technologies designed to identify synthetic media, manipulated biometric data and biometric injection attacks targeting remote identity verification systems and digital onboarding workflows.

P

Paravision

paravision.ai

Paravision is a private biometric identity and computer vision company founded in 2013 and headquartered in San Francisco, California, USA. The company develops facial recognition, identity verification and authentication technologies for government, border security, travel and enterprise applications.

Paravision applies advanced computer vision, facial biometrics and liveness technologies to help governments and enterprises detect spoofing attempts, synthetic identities, deepfakes and biometric injection attacks in high-security identity verification and authentication environments.

Persona

withpersona.com

Persona is a private identity infrastructure company founded in 2018 and headquartered in San Francisco, California, USA. The company provides configurable identity verification and fraud prevention solutions for online platforms and digital services.

Persona combines identity verification, liveness detection and fraud intelligence capabilities to help organizations detect deepfakes, synthetic identities and biometric injection attacks during remote onboarding and authentication.

Prove

prove.com

Prove is a private digital identity company founded in 2008 and headquartered in New York, USA. The company provides phone-centric identity verification, authentication and fraud prevention technologies for financial institutions, healthcare providers and digital service platforms.

Prove combines mobile identity verification, device intelligence and fraud prevention technologies to help organizations defend against account takeover attempts, synthetic identities and emerging digital fraud threats. Its platform leverages mobile network and device-possession signals to help establish trust during onboarding, authentication and high-risk transactions, complementing broader defenses against deepfake-enabled and injection-based fraud.

R

Reality Defender

realitydefender.com

Reality Defender is a private deepfake detection company headquartered in New York, USA. The company develops AI-driven technologies designed to identify synthetic audio, video and image content across digital channels.

Reality Defender's platform helps organizations detect AI-generated impersonation attempts and biometric injection attacks targeting identity verification, communications and authentication systems.

R

Regula

regulaforensics.com

Regula is a private identity verification and forensic technology company founded in 1992 and headquartered in Minsk, Belarus. The company provides document authentication, biometric verification and forensic examination technologies for governments, border agencies and commercial enterprises worldwide.

Regula combines document verification, facial biometrics and liveness detection technologies to help organizations detect deepfakes, synthetic identities and biometric injection attacks targeting remote identity verification systems.

ROC

roc.ai

ROC is a private computer vision and biometrics company founded in 2016 and headquartered in McLean, Virginia, USA. The company develops facial recognition and computer vision technologies for security, law enforcement and identity verification applications.

ROC provides facial biometric authentication and liveness technologies designed to help organizations defend against spoofing attempts and biometric injection attacks targeting remote identity systems.

S

Shufti

shuftipro.com

Shufti is a private identity verification company founded in 2017 and headquartered in London, UK. The company provides AI-driven identity verification, KYC and AML compliance technologies for businesses worldwide.

Shufti combines facial biometrics, document verification and liveness detection technologies to help organizations prevent deepfake fraud, identity spoofing and biometric injection attacks.

Signicat

signicat.com

Signicat is a private digital identity company founded in 2007 and headquartered in Trondheim, Norway. The company provides electronic identity, authentication and digital fraud prevention solutions for financial institutions and regulated industries.

Signicat offers identity verification and biometric authentication technologies designed to help organizations mitigate deepfake-enabled fraud, account takeover attempts and biometric injection attacks.

T

Thales

thalesgroup.com

Thales is a publicly traded aerospace, defense and digital security company founded in 2000 and headquartered in Paris, France. The company provides identity verification, biometrics and cybersecurity technologies for governments and enterprises worldwide.

Thales develops biometric authentication and liveness detection technologies designed to help organizations protect against spoofing attempts, synthetic identities and biometric injection attacks.

Trulioo

trulioo.com

Trulioo is a private identity verification company founded in 2011 and headquartered in Vancouver, Canada. The company provides global identity verification, business verification and fraud prevention technologies for financial institutions, marketplaces and digital platforms.

Trulioo combines identity verification, biometric authentication and fraud prevention capabilities to help organizations combat synthetic identity fraud, deepfake-enabled attacks and biometric injection attempts during remote onboarding.

U

Unico

unico.io

Unico is a private digital identity and biometric authentication company founded in 2007 and headquartered in São Paulo, Brazil. The company provides biometric verification, authentication and fraud prevention technologies for financial services, government and enterprise customers.

Unico combines facial biometrics, liveness detection and fraud prevention technologies to help organizations defend against spoofing attempts, deepfakes and biometric injection attacks across onboarding and authentication workflows.

Unissey

unissey.com

Unissey is a private biometric identity verification company headquartered in Switzerland. The company provides biometric authentication, identity verification and fraud prevention technologies for financial institutions, digital service providers and regulated industries.

Unissey combines facial biometrics, liveness detection, Presentation Attack Detection (PAD) and Injection Attack Detection (IAD) technologies to help organizations defend against deepfakes, virtual cameras, synthetic identities and biometric injection attacks. Its platform is designed to support secure remote onboarding and authentication by helping ensure that biometric data originates from a genuine user and trusted capture environment.

V

Veriff

veriff.com

Veriff is a private identity verification company founded in 2015 and headquartered in Tallinn, Estonia. The company provides AI-powered identity verification and fraud prevention technologies for online businesses and regulated sectors.

Veriff combines facial biometrics, document authentication and liveness detection to help organizations detect deepfakes, synthetic identities and biometric injection attacks during remote onboarding.

Y

Yoti

yoti.com

Yoti is a private digital identity company founded in 2014 and headquartered in London, UK. The company develops identity verification, age assurance and biometric authentication technologies for businesses and governments.

Yoti's platform incorporates facial biometrics and liveness detection technologies designed to help organizations defend against deepfakes, presentation attacks and biometric injection attacks.

Youverse

youverse.id

Youverse is a private digital identity company headquartered in Portugal. The company provides decentralized identity verification and biometric authentication technologies focused on privacy-preserving digital identity solutions.

Youverse combines biometric verification, liveness detection and AI-powered anti-spoofing technologies to help organizations mitigate synthetic identity fraud, deepfakes and biometric injection attacks in digital onboarding and authentication environments.

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS