iProov

Threat Intelligence Report 2026

The Fifth Industrial Revolution is defined by human–machine collaboration. But the same technologies driving creativity and scale have also industrialized deception, enabling bad actors to move faster than ever and putting digital trust at the center of the modern economy.

The industrialization of deception whilst rife in identity proofing, is now also targeting daily video calls that underpin corporate governance. As executive impersonation becomes a turnkey operation, the video conference has emerged as a primary vector for systemic operational risk.

We are currently operating on an uneven playing field with bad actors leveraging the hard skills of AI superhuman analytical speed, perfect mimicry, and rapid reconnaissance to exploit our unaugmented human soft skills. Traditional cybersecurity defenses were not designed to detect real-time synthetic media injection.

The Identity Industry's Injection Blind Spot

The identity industry is currently hamstrung by a dangerous misconception that this report aims to dismantle: **the belief that injection attacks, such as deepfakes, are either hyped or easily mitigated.**

The blind spot is exacerbated by two critical market failures:

1. A market saturated with unverified efficacy, where vendors claim extensive mitigation without a common framework or baseline to prove it. This results in what can be described as security theatre, where the perceived defense is far greater than the technical reality.
2. A reliance on point-in-time certifications as proof of resilience. Organizations are mistaking a static certification for an active defense, failing to realize that a standards-aligned test is the starting line, not the finish line, in an environment of daily Tactics, Techniques, and Procedures (TTP) evolution.

A Strategic Reckoning

This report is not based on theoretical models; it is built from real-world telemetry via the iProov Security Operations Center (iSOC) and our specialized Threat Intelligence teams. We are seeing a relentless evolution of Tactics, Techniques, and Procedures (TTPs) that traditional static defenses simply cannot detect.

Organizations must validate vendor performance through independent measured outcomes rather than relying on marketing claims or historical certifications. When defenses are not continuously tested against injection techniques, attackers can bypass controls without detection. To close this gap, organizations must move past the compliance checkbox processes. A one-time certification doesn't mean much when the attackers are evolving every hour. Security programs must account for continuous threat evolution rather than relying on periodic certification.

A Scientific Framework for Defense

Through our collaboration with **MITRE on the ATLAS Framework**, we categorize threats not by their novelty, but by their reality: **Feasible, Demonstrated, and Realized.**

In the following pages, we move past the fluff of industry buzzwords to reveal the actual TTPs used by global groups to commit industrialized fraud.

Dr. Andrew Newell
iProov Chief Scientific Officer

2026 Trends

iProov

Trend 1: Criminals Without Borders

Regional security strategies are now a liability. Large organizations that deploy different vendors, varying detection thresholds, and disconnected response protocols across territories are creating exploitable seams.

The mistake organizations are making is assuming local threats stay local. Sophisticated threat groups no longer see your organization as a series of regional offices. They see a single, interconnected ecosystem with specific vendor weak spots. By targeting the weakest link in a multi-vendor chain, attacks can compromise a global identity network from a single entry point.

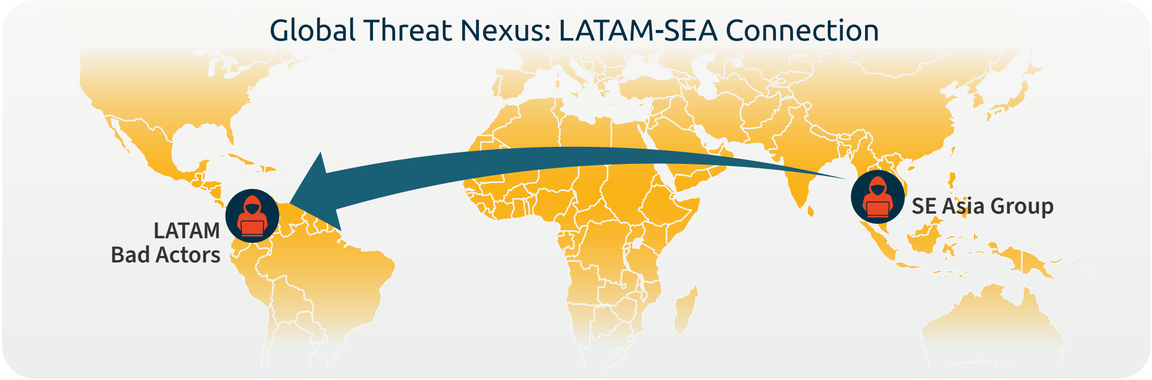
Attackers are now hyper-collaborative, sharing Tactics, Techniques, and Procedures (TTPs) across borders with near-instantaneous speed. A breach method perfected in Southeast Asia today becomes a Latin America playbook tomorrow and vice versa.

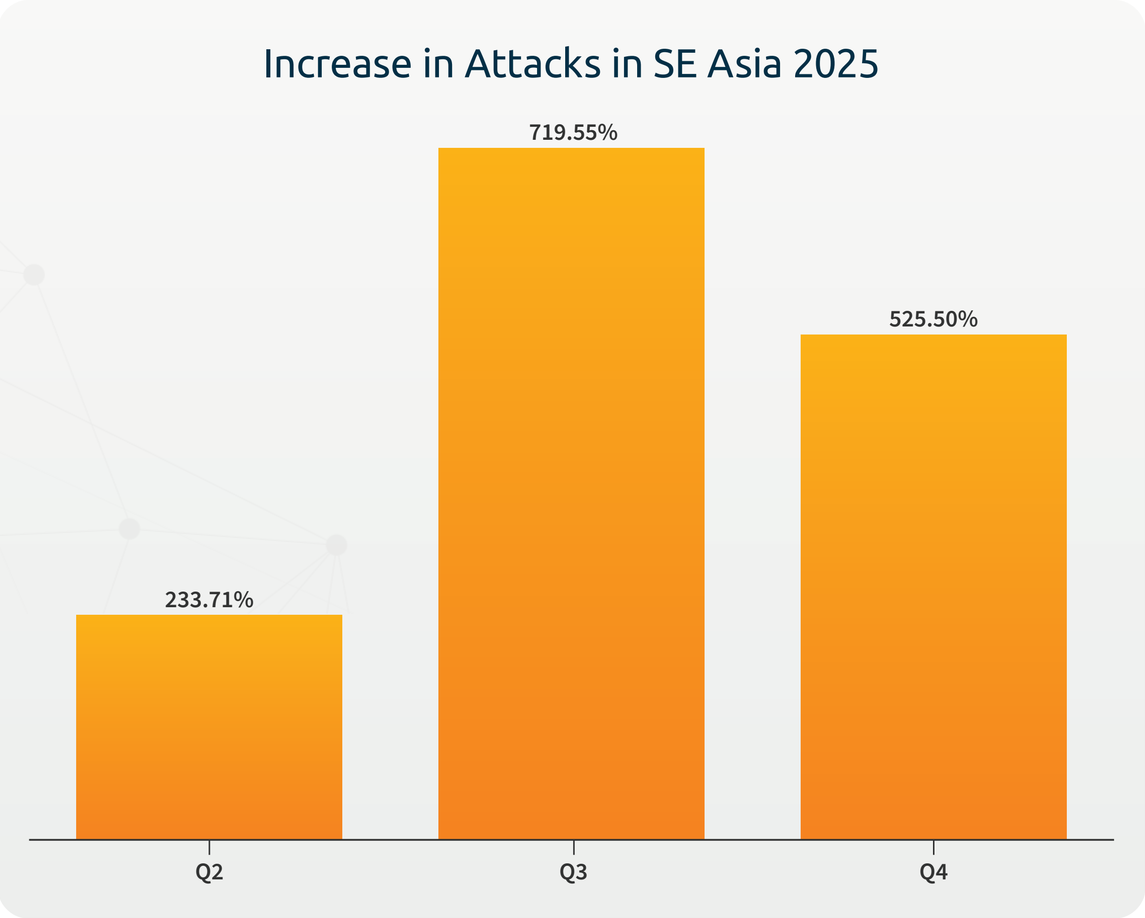
The rapid surge in Southeast Asian attacks is not a coincidence; it is the direct result of a transition from open-source experimentation to professionalized criminal infrastructure. Our intelligence has tracked a specific, high-velocity evolution within these cross-border groups.

What began as public projects on GitHub has been privatized by Chinese-speaking groups into sophisticated, closed-source product development. These groups now weaponize frameworks like Xposed to hook into Android systems, allowing them to intercept and manipulate device data at the root level.

We have identified a direct tactical link between the proliferation of virtual camera technologies emanating in Southeast Asia and being shared and utilized by specialized LATAM threat groups targeting financial institutions. Back in 2023, these groups were limited to sharing basic PDF guides for manual presentation attacks. By 2024, they had industrialized their operations, deploying CraxsRAT malware. Allowing them to bypass weak biometric liveness technology entirely by exfiltrating login credentials and hijacking live camera feeds in real-time.

In 2025, we observed groups in Southeast Asia pivoting from distributing cracked Android Package Kits (APK) files to releasing high-value KYC data packages. These bundles include stolen U.S. and European identity documents, with matching selfies. This isn’t an isolated incident of collaboration and specific targeting; it is on its way to becoming the norm. This cross-hemisphere collaboration has created a synchronized threat environment where Southeast Asian groups effectively beta-test the innovations that LATAM groups later industrialize. The current escalation in Southeast Asian attack volumes is a direct lead indicator for the professionalized offensive we now expect to see across Latin American financial institutions.





Key Takeaway: Utilizing a patchwork of different security vendors across regions creates dangerous silos that lack centralized intelligence. When one region identifies a new TTP, the other regions remain blind if they are on different platforms. Security architectures that don't take a global view will create weak spots which become the primary target and entry point for globalized fraud campaigns. Managed detection and response must be global by design.

Target: Financial Services, Crypto globally

Motivation: Monetary gain.

Trend 2: The iOS Security Gap

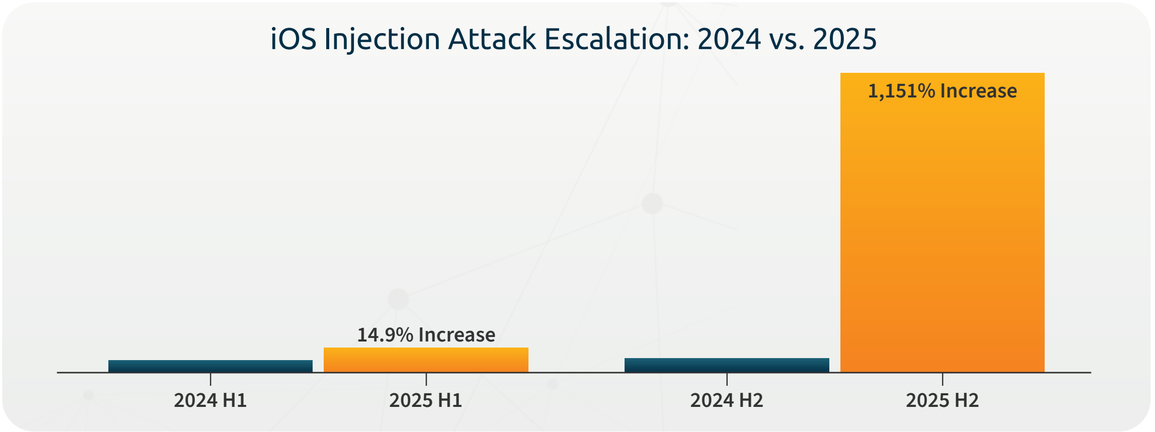
Injection attacks started on web platforms, moved to Android, and for years, iOS stayed relatively untouched. The perceived robustness stemmed from Apple's closed-loop of owning the entire stack, from the hardware to the operating system and App Store. Apple could enforce absolute control over the security and usability. In contrast, Android's open-source nature requires it to be a universal operating system, working across thousands of diverse, often low-spec device types. To ensure this broad accessibility, Android historically made compromises in fragmentation and hardware-level isolation, making it an easier initial target. Security teams, lulled into a false sense of security by Apple's control, highlighted the platform as low-risk. That assumption is now dangerous.

In September 2025, our threat intelligence team found a highly specialized iOS video injection tool that changes how we need to think about identity fraud on iOS devices. This tool is purpose-built as a part of a crime infrastructure designed for programmatic, scalable attacks against identity verification.

The iOS video injection tool works on jailbroken iOS 15 and later devices. Because generating hyper-realistic deepfakes requires the massive GPU power of a desktop workstation that mobile hardware cannot yet support, attackers utilize a Remote Presentation Transfer Mechanism (RPTM) server. This allows them to offload the heavy AI processing to a remote computer, then inject the finished high-fidelity video directly into the device's video stream. The injection occurs before the camera layer, bypassing the physical camera entirely and presenting the application with a legitimate-looking, real-time feed.

While current observations of this tool are limited to jailbroken iOS 15+ environments, this is merely the incubation phase. The technical architecture of RPTM serves as a blueprint for the next generation of injection attacks. The jump to standard, non-jailbroken devices is 'Version 2.0' of this threat, and is already underway. As attackers move towards lower-level instruments, it means we are no longer looking at a niche exploit, but the industrialized beta-testing of a platform-wide vulnerability.

The H2 Escalation: While H1 saw a modest year-over-year increase of 14.9%, the second half of 2025 (H2) experienced a critical surge of 1,151% compared to the same period of 2024. This hyper-growth in Q3 and Q4 marks the transition from experimental testing to the full-scale industrialization of iOS injection attacks.



Key Takeaway: We are beginning to observe that threat actors have already adjusted their strategy to focus on iOS. What was once safe is now the primary target. Security plans built on the idea that iOS provides inherent protection need immediate review. Exploitation is already underway. In several regions, we have observed this shift accelerate within a single quarter.

Target: All industries and regions are vulnerable. This is the new battleground and requires urgent attention.

Motivation: Monetary gain

Trend 3: The Scaling of Virtualized Attacks

The barrier to entry for high-fidelity identity fraud has collapsed. We are now witnessing the emergence of the fraud, where low-skilled, opportunistic individuals can execute sophisticated attacks using inexpensive tools. This is a scalability breakthrough for criminal groups and nation-states. By moving from cumbersome local software to scalable cloud environments, attackers have turned identity fraud into a repeatable, high-volume, turnkey criminal operation. Previously, it was a single bad actor who was limited by the number of physical devices they owned, launching hundreds of simultaneous attacks from a single laptop. Today, an army of incentivized individuals can attack your platform with readily available, inexpensive tools.

In the past, an attacker needed a physical device and deep technical knowledge to spoof a biometric check. Today, they use cloud emulators (a virtual mobile phone) that run inside a standard web browser tab.

1. The attacker accesses a virtual phone in the cloud and can modify its system files to make it look like a legitimate, high-end Android device to avoid detection.
2. Instead of using a physical camera, they use Virtual Camera software, which acts as a digital bridge, allowing them to stream high-quality deepfakes directly into the verification application.
3. These tools are so efficient that they have almost no lag (under 1.5 seconds). This allows the attacker to react in real-time to an active liveness prompt, like nodding or smiling, making the fake video appear like a live human is genuinely present. This interactive process is known as hill climbing, allowing attackers to programmatically test and refine different media variants until they find the specific iteration that successfully passes the biometric threshold. Essentially, this approach now makes liveness that uses active challenge responses obsolete.

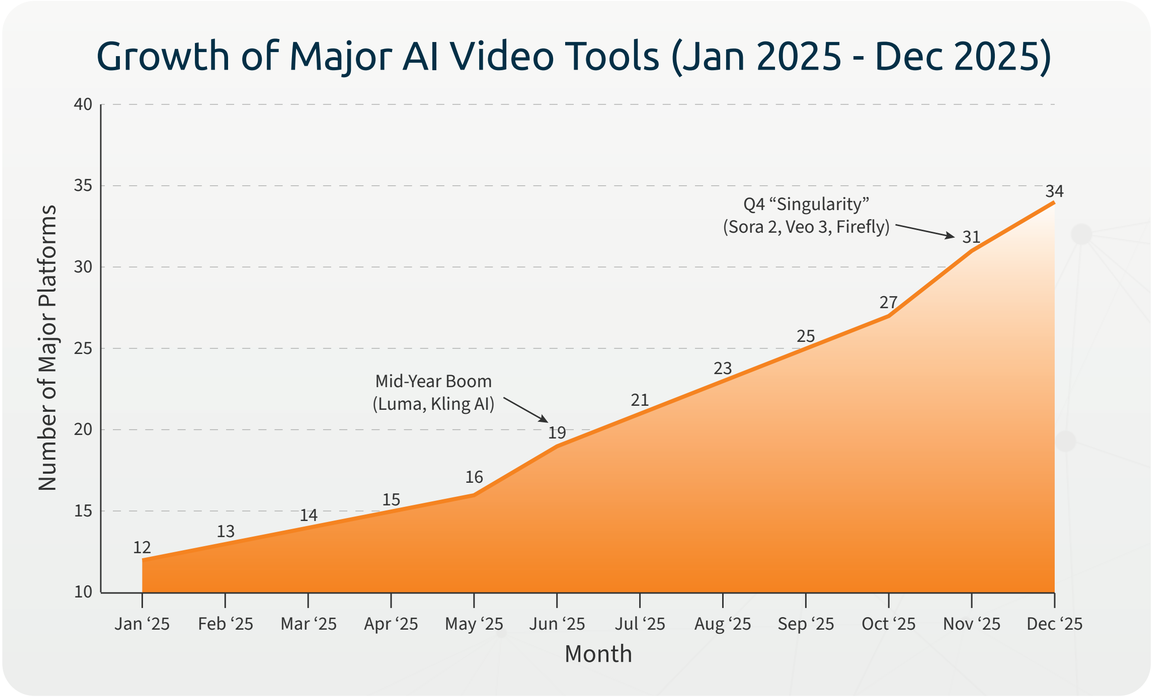
With virtualized environments mimicking legitimate devices, the trusted device narrative is dead. Traditional device fingerprinting fails to flag these as fraudulent, and a common misconception is that Endpoint Detection and Response (EDR) will fill the gap. In reality, while EDR secures the enterprise perimeter, it is entirely blind to the integrity of the biometric data stream. As non-technical bad actors flood the market with stolen KYC data packages and selfies, the volume of synthetic identity fraud will overwhelm manual review processes, leading to catastrophic failures in regulatory non-compliance and financial loss.

To counter the Scaling of Virtualized Attacks, many organizations are falling into a complexity trap, layering disjointed bolt-on security tools that increase technical debt and operational costs, while leaving invisible cracks between non-integrated or centrally monitored systems. This fragmented defense ultimately fails to stop sophisticated injection attacks, leading to an explosion of manual reviews and potentially catastrophic regulatory exposure.

Key Takeaway: Since virtualized hill climbing attacks have rendered the trusted device narrative obsolete, organizations must move beyond disjointed security bolt-ons towards a unified Managed Detection and Response (MDR) framework. Only a continuous loop, combining orthogonal automated layers with active human oversight, can bridge the invisibility gaps between systems and neutralize injection attacks in real-time.

Trend 4: PREDICTION: Hyperrealistic Deepfakes

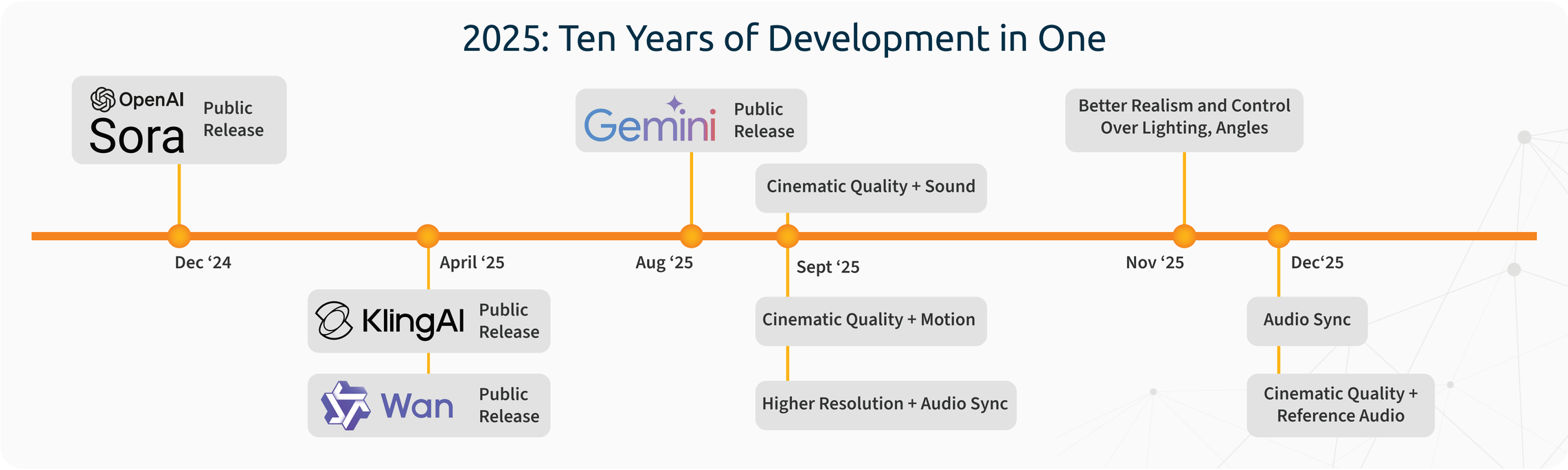
The era where “seeing is believing” has ended. The rapid intensification of image-to-video conversion tools (which we warned about in our Threat Intelligence Report 2025) has created a crisis that extends beyond simple identity fraud to systemic operational risk. As well as spoofing weak liveness checks, attackers use faceswaps to impersonate C-suite executives and critical vendors in real-time video calls. When a single convinced interaction can trigger a supply-chain collapse, visual identity becomes the primary point of systemic risk.



While early deepfakes required vast datasets of a victim’s likeness, modern First Order Motion Models (FOMM) have lowered the barrier to zero. This AI framework brings a still photo to life by borrowing movements from a separate video, mapping expressions and gestures directly onto a victim’s image.

- **The Single-Image Attack:** Using just a photo from a driver’s license or LinkedIn profile, an attacker can generate a fully animated video stream.
- **Motion Reenactments:** These tools allow an operator to map their own facial expressions, such as blinking, smiling, or speaking onto the victim’s static image in real-time.
- **Human vs. Machine:** These deepfakes are designed to deceive the human eye during Zoom or Team calls.

Traditional FOMM attacks are often pre-recorded or lack a realistic 3D effect, making them detectable by advanced biometric analysis. The emergence of image-to-video conversion tools, such as Nano Banana, Sora 2, and Kling AI 2.6 solve these limitations by moving away from tweaking flat photos to simulating how real light and movement work in 3D, ensuring the digital face remains stable and hyper-realistic throughout a live interaction. See how this looks in reality.



The Forecast:

This year, we predict that these hyperrealistic, live deepfakes applied directly to an attacker’s face during a video conference meeting will become a primary target.

This would allow an attacker to not just play a video, but to become the victim during a live interaction, easily fooling human reviewers and neutralizing many current liveness solutions challenges. Active liveness solutions that require a movement or action will be easily duped, and those organizations that fail to deploy solutions with multi-layered defenses, where the vendor captures a broad range of signals from the user, imagery, and device for high accuracy and security, will remain vulnerable.

The transition from theoretical threat to operational catastrophe is already underway and documented. In 2024, the engineering giant Arup suffered a staggering $25m loss after an employee in Hong Kong was deceived during a video call in which every participant, including the CFO, was a deepfake digital recreation. This was followed in 2025 by a sophisticated attempt to impersonate the CEO of WPP, Mark Read, via a Microsoft Teams call, using voice and video to solicit funds and sensitive data. These cases prove that attackers are no longer just targeting entry-level KYC; they are leveraging human-to-human trust to execute high-value wire fraud and bypass corporate governance through the very video platforms we rely on for daily business.

In Gartner's Rising Tide of Deepfake Attacks Study (September 2025), cybersecurity leaders revealed that deepfake incidents are increasingly impacting organizations, with 37% experiencing deepfakes in video calls. This mirrors The Ponemon Institute research, which shows 41% of organizations saw deepfake impersonation of executives, an increase from 34% previously.

Key Takeaway: Relying on visual verification by human staff is no longer a viable security control. Convincing impersonations of leadership can lead to unauthorized fund transfer or the release of sensitive data. Organizations must transition from matching a face to a photo to verifying genuine human presence. Security must evolve to ensure the user behind the screen is a real person presenting in real-time, not a synthetic puppet.

Target: All video conferencing platforms.

Standards-Aligned Testing is the Foundation of Objective Evidence

The threat landscape has clearly moved from Presentation Attack Detection (PAD), stopping physical masks or photos, to Injection Attack Detection (IAD), and stopping digital compromise. While novel attack methodologies are shared instantly in criminal communities, the industry has historically lacked a common language to measure vendor resilience.

This is where standards become critical. Standards define measurable control objectives and test methodologies. Certification alone does not guarantee ongoing performance if testing conditions do not reflect current injection techniques.

Major cybersecurity authorities, including NIST, the French ANSSI, German BSI, and European ENISA have identified injection attacks as a critical risk. In response, a new architecture of guidelines and standards now defines the minimum threshold for vendor resilience in this new landscape.

The Key Standards & Guidelines to Recognize

NIST SP 800-63-4: The Global Benchmark

NIST introduced an entirely new set of Digital Identity Guidelines in 2025, NIST SP 800-63-4. One of the key components is an update to account for sophisticated AI-driven attacks. Protection against injection attacks is now a mandatory control objective for higher assurance levels and for continuous authentication of a user throughout the lifecycle. A marked shift from static identity proofing to adaptive defenses to mitigate injection attacks. The emphasis on continuous evaluation and performance metrics, including authentication failure rates and new AI and ML documentation requirements, ensures organizations can adapt as fraud tactics evolve and build long-term trust with users.

Standards-Aligned Testing vs. Vendor Claims

FIDO Face Verification Certification: FIDO Certification mandates a dual-standard audit, it bridges the gap between ISO 30107-3, which measures resistance to presentation attacks (IAPAR), and ISO 19795, which benchmarks biometric performance and accuracy (FAR/FRR). By requiring independent laboratory testing across thousands of transactions, FIDO ensures that a system's defensive posture does not come at the expense of usability or demographic inclusivity. It represents the industry's first certification that validates both security and performance in a single, auditable framework.

CEN/TS 18099: Many vendors claim they can detect injection attacks without providing third-party standards-aligned evidence to support such claims. However, with unproven defenses, you open the door to account takeover, identity fraud, and financial crime at scale. CEN/TS 18099 is the new technical specification designed to assess a biometric system's resistance to injection attacks. It provides a solid baseline that organizations can reliably measure their risk exposure against. Organizations procuring CEN-evaluated solutions gain auditable proof of injection attack detection that aligns with NIST SP 800-63-4, however, real-world performance will still depend on deployment configuration and threat monitoring practices.

ISO 25456: Biometric Data Injection Attack Detection
ISO 25456, expected in 2027, will formalize injection attack testing at an international level.
While CEN/TS 18099 was the start, this new standard provides a certifiable test plan. It demonstrates clear, auditable proof of a vendor's robustness to injection attacks. This new standard puts the burden of proof on the vendor, and provides confidence to procuring organizations.

Andrew Bud
Founder and CEO, iProov

"Attack techniques now spread globally in days. Point-in-time compliance is not sufficient in this environment. Organizations need continuous monitoring, regular validation, and the ability to respond quickly as threats evolve."

From Standards to Action: The Operational Feedback Loop

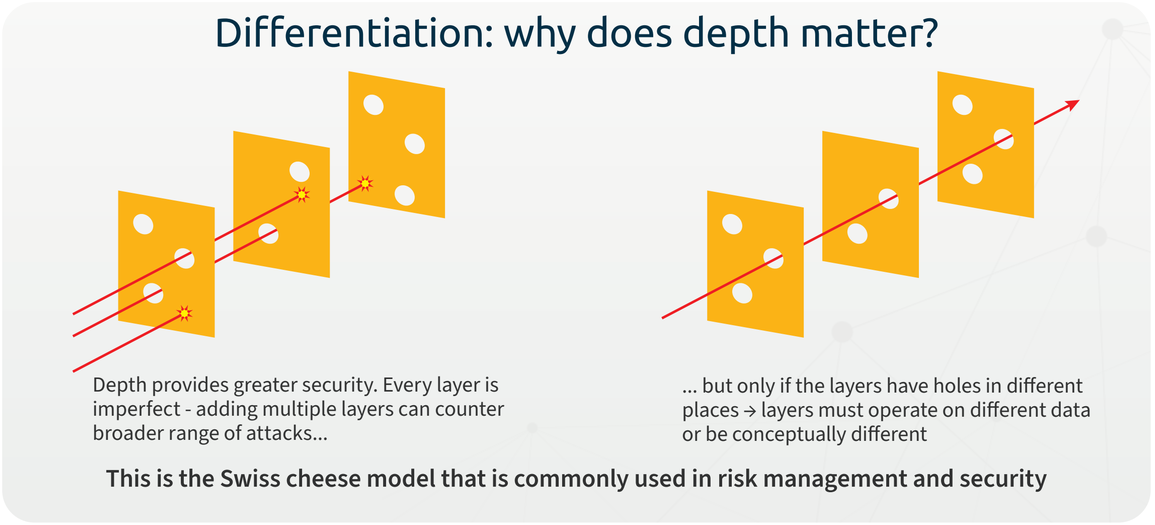
Organizations must move beyond a “moment in time” compliance checklist towards active validation. A proactive, built-in security approach and Security by Design ensures that systems are resilient from the point of requirement definition, rather than relying on reactive bolt-ons that increase technical debt.

To operationalize the trends and standards identified in this report, iProov leverages a continuous cycle of managed detection and response:

- **Threat Intelligence:** This is the early warning system that turns raw darknet data into actionable insights. By identifying specific TTPS (Tactics, Techniques and Procedures) as they emerge, we can move from generic alerts to strategic foresight.
- **Red Team Testing:** We do not wait for an exploit to test our defenses. Red Teams emulate real-world adversaries to proactively uncover and fix vulnerabilities before they are exploited. This validates that security controls are not just present, but configured and operating effectively against live threats.
- **iProov Security Operations Center (iSOC):** Provides the continuous monitoring required by NIST SP 800-63-4 When new threats are identified via intel or red teaming, iSOC rapidly deploys countermeasures to ensure ongoing protection.

Building Orthogonal Resilience Through Managed Detection and Response

A multi-layered approach requires redundancy without replication, the layers should be orthogonal, meaning they must function in fundamentally different ways to achieve a “Swiss Cheese” model of defence. Whilst every individual security layer has inherent holes or vulnerabilities, stacking orthogonal defenses ensures these gaps do not align. Even if a sophisticated AI exploit penetrates one layer, the attack is neutralized by the next layer.



Because the threat landscape is not static, your defense cannot be either. The final, critical layer is MDR. While the multi-layers handle the millisecond-level detection, the iSOC provides the intelligence loop. By monitoring global attack patterns, we don’t just detect attacks; we anticipate their evolution. This combination of orthogonal automated layers and human-led threat intelligence creates the continuous defense that adapts faster than the adversaries can innovate.

Securing the 5th Industrial Revolution

Identity systems are now operating in an environment where injection attacks are scalable, automated and globally coordinated. This brings a new industrialised attack surface where identity is the primary battleground.

As we have seen throughout this report, the threats of 2026 are no longer static or regional. The trends we've identified, from the **Criminals Without Borders** to the **iOS Injection Security Gap**, demonstrate that attackers are sharing attack methodologies and focusing on areas that once seemed impenetrable. High-profile losses, such as the $25m Arup case prove that human visual verification is no longer a viable security control for live business interactions. Organizations must now move past simple credential matching to unquestionably determine genuine human presence in remote meetings. The arrival of clear frameworks such as NIST SP 800-63-4 and standards like CEN/TS 18099, signpost towards the proof of resilience of injection attacks.

To stay ahead, organizations must move beyond retrospective compliance to the integrated operational feedback loop. This requires shifting away from self-certified marketing claims in favor of standards-aligned injection attack detection backed by Managed Detection and Response. We've seen that trust has been compromised, and therefore security must evolve from simply verifying credentials to unquestionably determining whether a real person is genuinely present during the verification process. Organizations that integrate injection attack testing, continuous telemetry analysis, and independent standards validation will materially reduce exposure to synthetic identity fraud.

Threat Intelligence 2026 Webinar