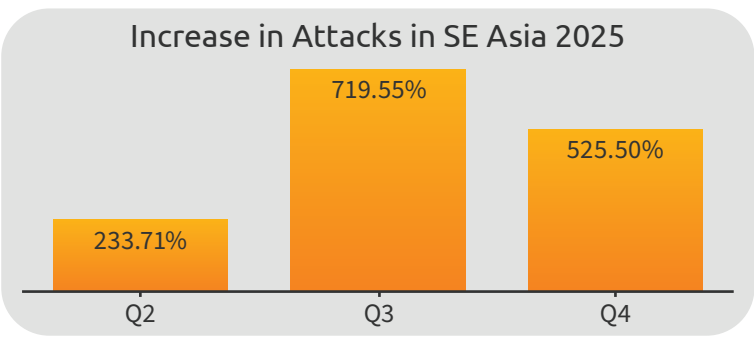
iProov Threat Intelligence Report 2026: Identity is the Primary Battleground

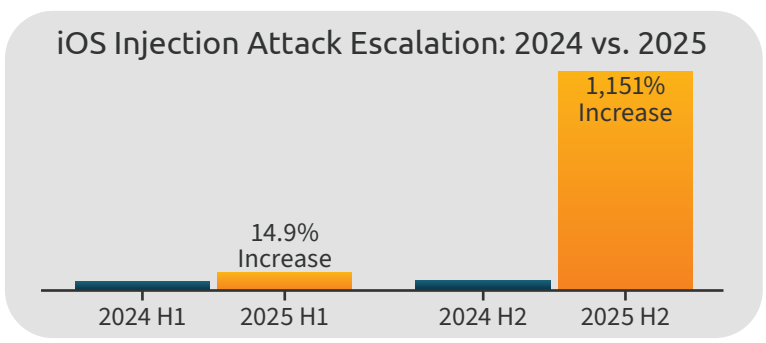
Traditional cybersecurity defenses were not designed to detect real-time synthetic media injection, leaving the industry hamstrung by a dangerous misconception that these attacks are easily mitigated.

Key 2026 Threat Intelligence

1. Criminals Without Borders:

Regional security strategies are now a liability as hyper-collaborative threat groups share Tactics, Techniques, and Procedures (TTPs) with near-instantaneous speed. Southeast Asian (SEA) groups effectively beta-test innovations that LATAM groups later industrialize.





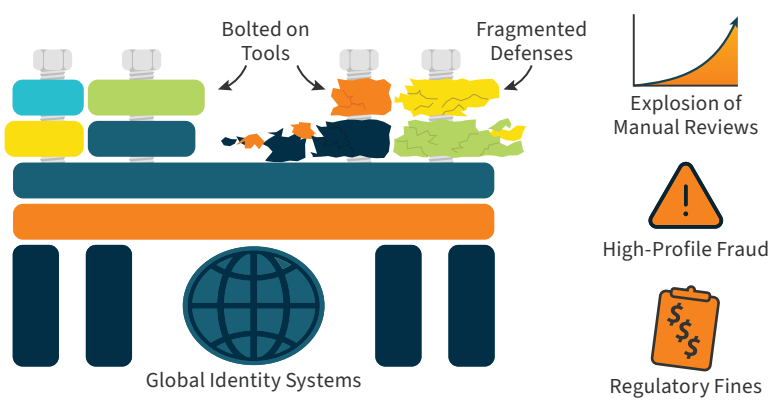
2. The iOS Security Gap:

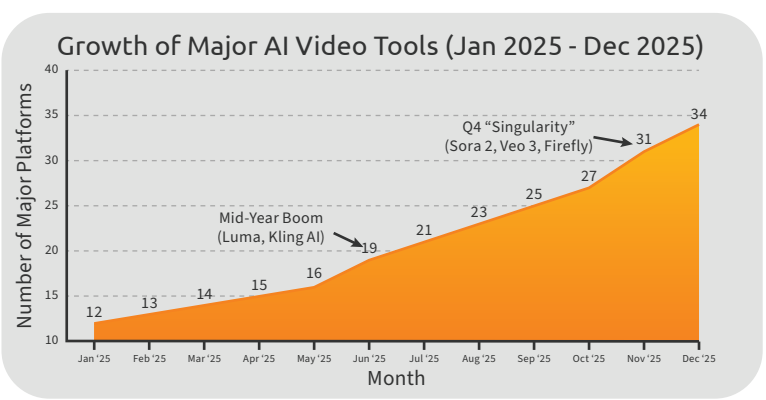
Apple's closed-loop ecosystem is now a high-velocity vulnerability, marking the industrialization of a previously ignored blind spot. While H1 2025 saw a 14.9% increase, **H2 2025 experienced a critical surge of 1,151% as attacks moved from experimental to industrialized.**

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

3. The Scaling of Virtualized Attacks:

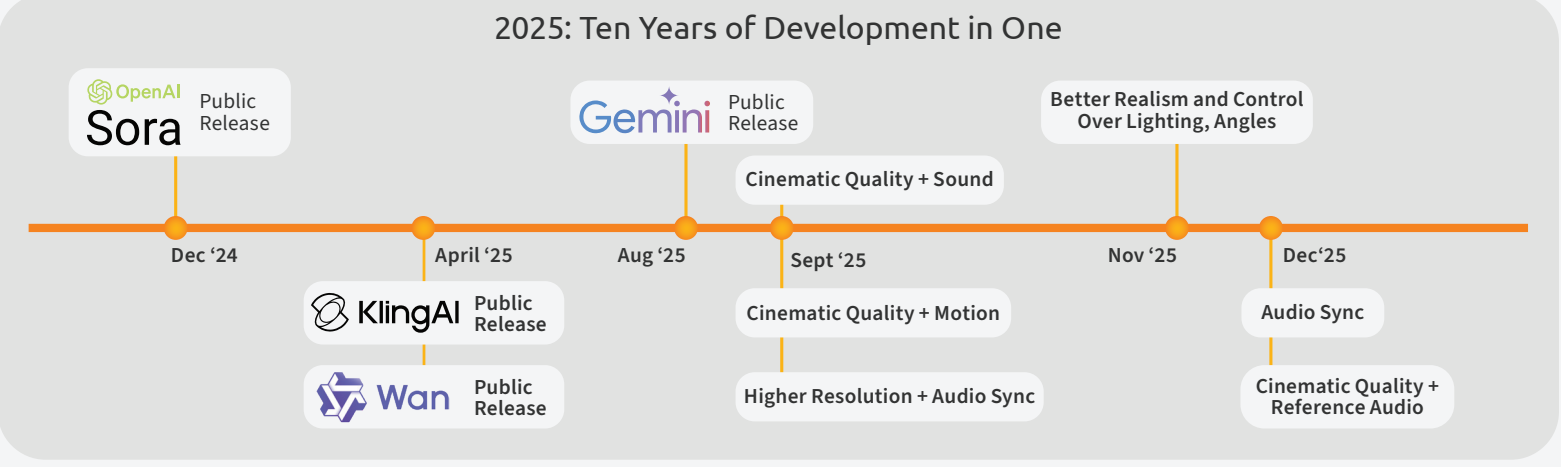
Organizations are falling into a complexity trap by layering disjointed, bolt-on security tools across different regions. This fragmented approach creates exploitable seams and technical debt, as patchwork regional defenses become the primary target and entry point for globalized fraud campaigns.





4. Hyperrealistic Deepfakes:

The primary concern has shifted to the rapid intensification of image-to-video conversion tools (such as Nano Banana, Sora 2, and Kling AI), which allow attackers to generate fully animated video streams from a single static photo.



37% of organizations experiencing deepfakes in video calls

Gartner's Rising Tide of Deepfake Attacks Study

41% of organizations saw deepfakes impersonation of executives

The Ponemon Institute research

The Framework for Resilience

Standards is the starting line. Organizations must move past marketing claims toward independent, measured outcomes.

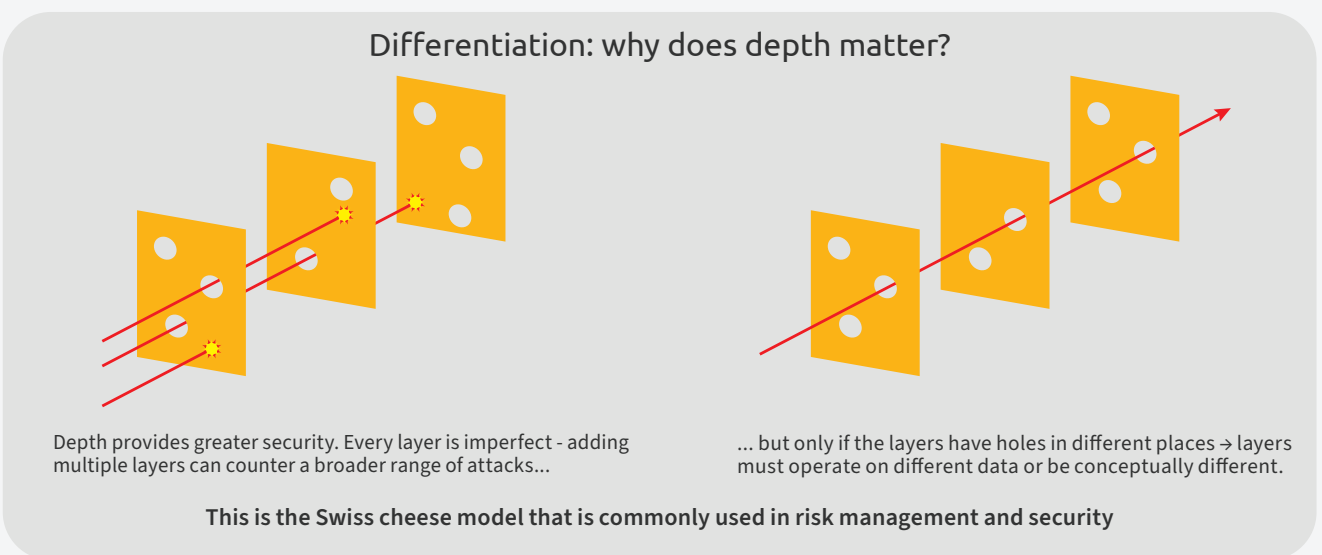
NIST SP 800-63-4: Protection against injection attacks is now a mandatory control objective for higher assurance levels.

CEN/TS 18099: Provides a solid baseline for assessing a biometric system's resistance to injection attacks.

FIDO Face Verification: The first certification to validate both security (IAPAR) and biometric performance (FAR/FRR) in a single framework.

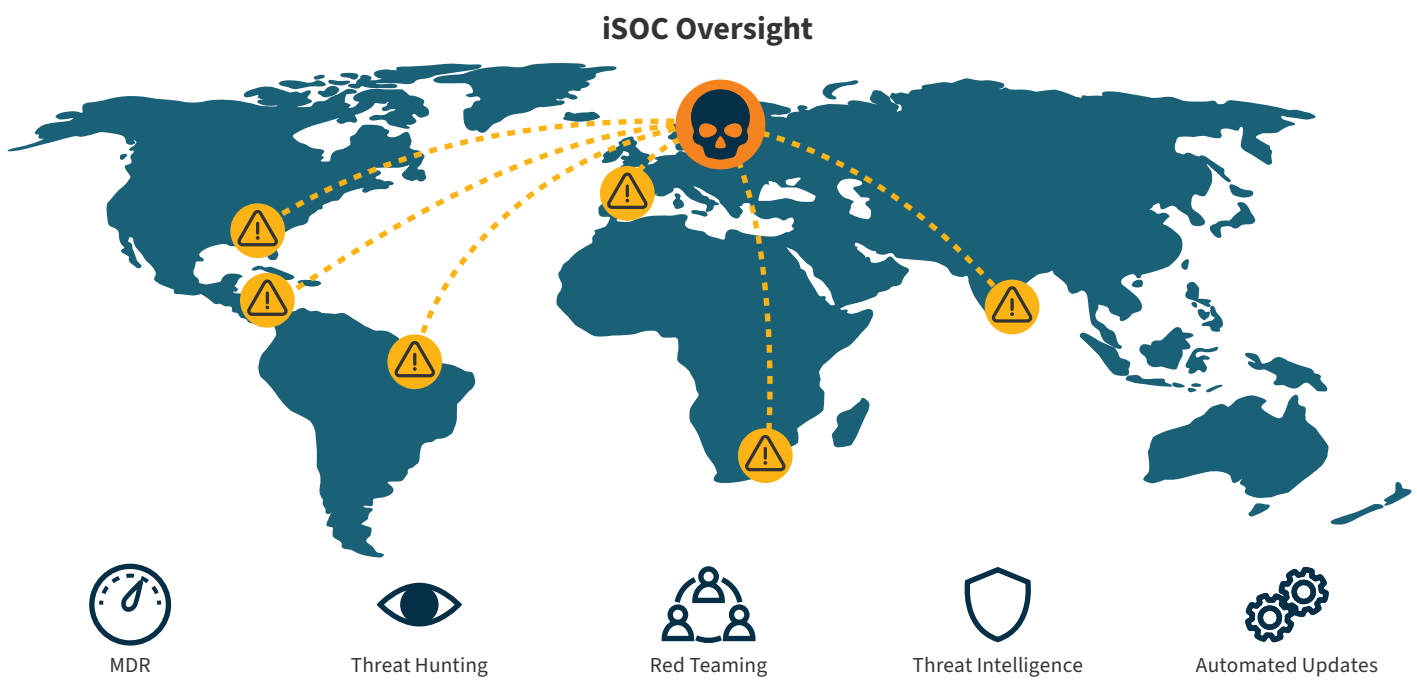
Orthogonal Defense & Active Validation

Defenses must function in fundamentally different ways—stacking layers so that inherent vulnerabilities do not align, following a "Swiss Cheese" model.



Managed Detection and Response (MDR)

While automated layers handle millisecond-level detection, the iProov Security Operations Center (iSOC) provides the continuous intelligence loop required to outpace adversaries.



Why does this matter?

In a world of increasingly sophisticated identity attacks, static defenses will fail. Success requires dynamic defenses and iSOC oversight powered by MDR, Threat Hunting, Red Teaming, Threat Intelligence, and Automated Updates.

Identity systems are now operating in a high-velocity environment where injection attacks are scalable, automated, and globally coordinated. This has created an industrialized attack surface where identity is the primary battleground. The threats of 2026 are no longer static or regional; they are sophisticated, hyper-collaborative, and focused on areas once deemed impenetrable.

Watch the on-demand **Threat Intelligence 2026 Webinar**