



May 20 - 22, 2026 | Austin, Texas, USA

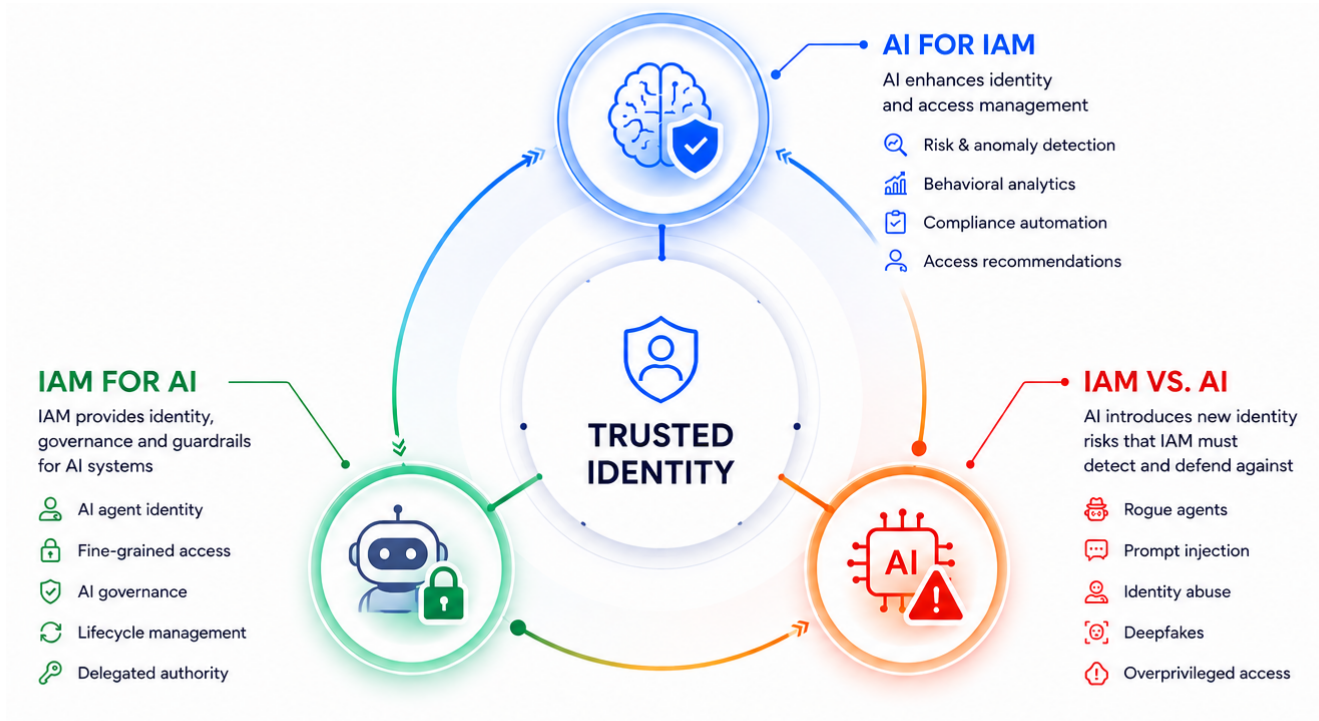
# The Evolution of IAM in the AI Era



**Johann Nallathamby**

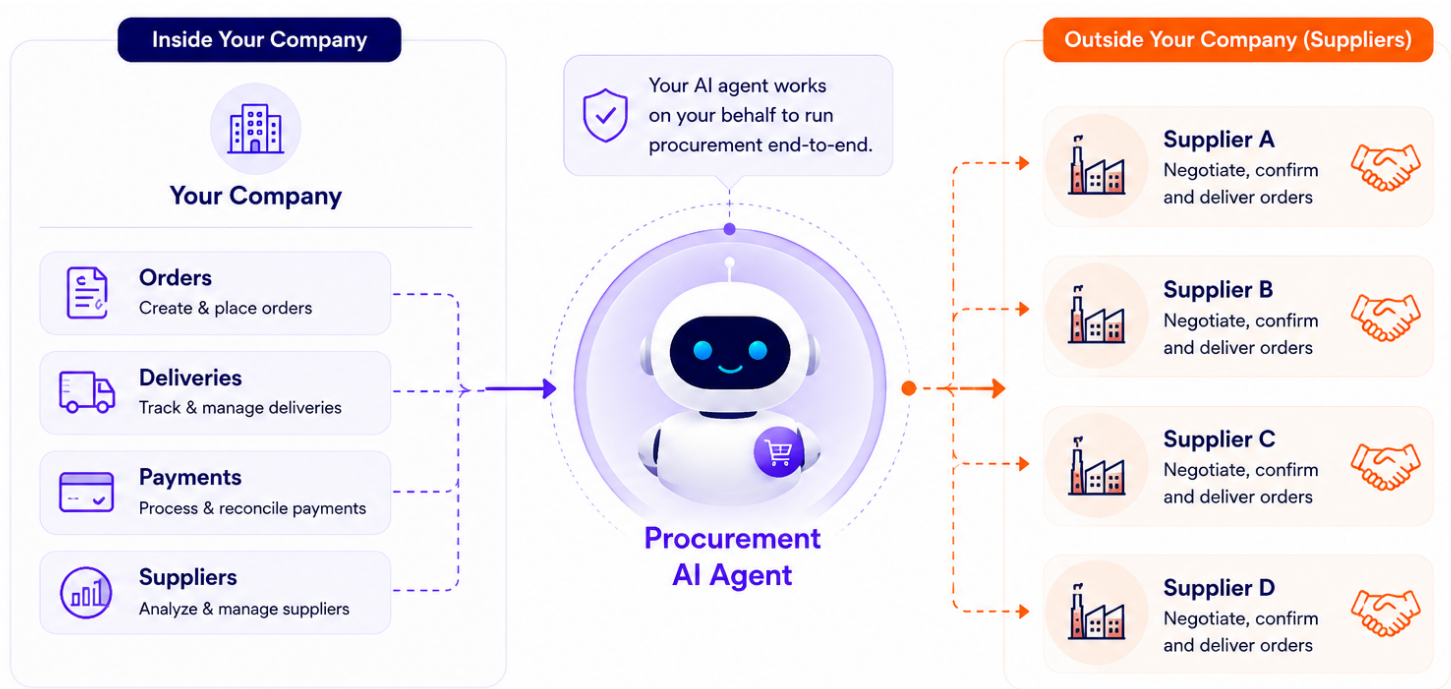
Senior Enterprise Architect & Field CTO

# The IAM-AI Triad



# IAM for AI

# IAM for AI

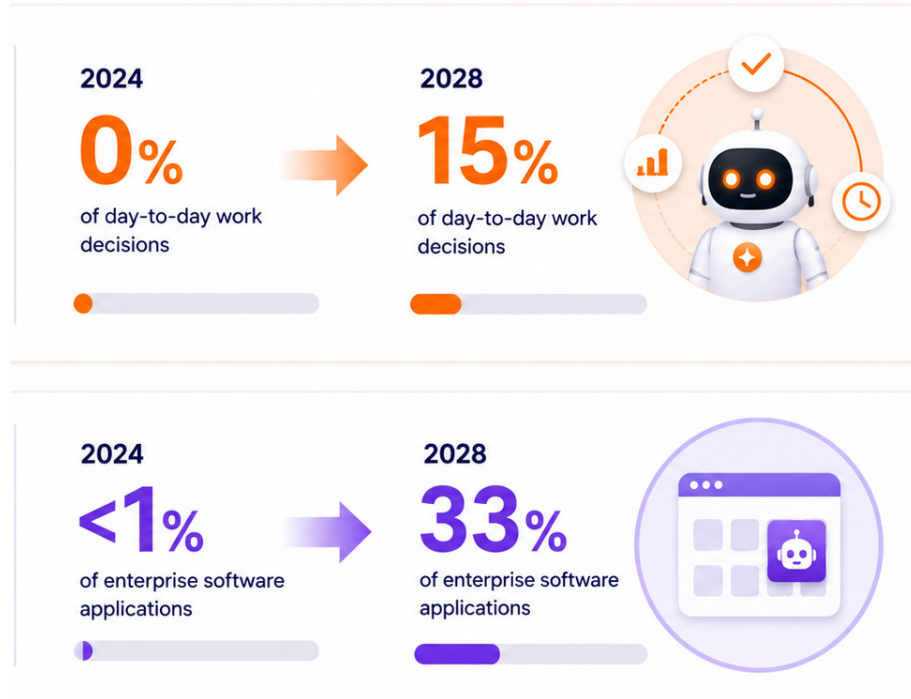


Your next multi-million dollar customer could be an AI Agent



# AI is changing the enterprise landscape!!

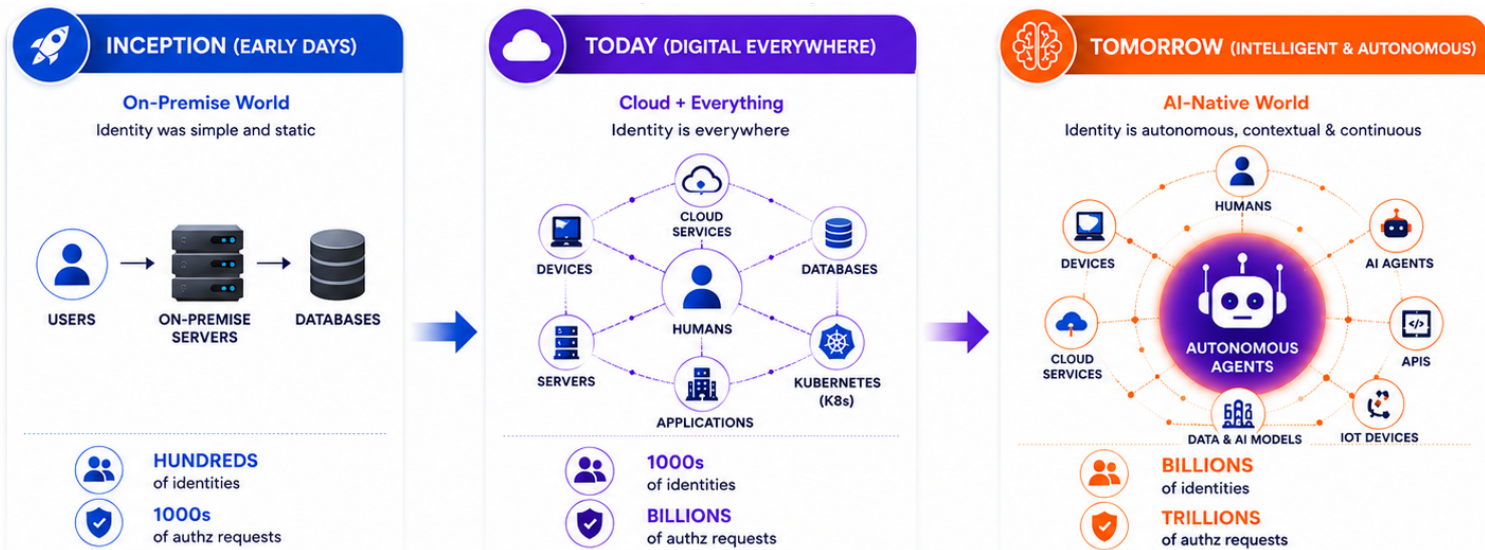
---



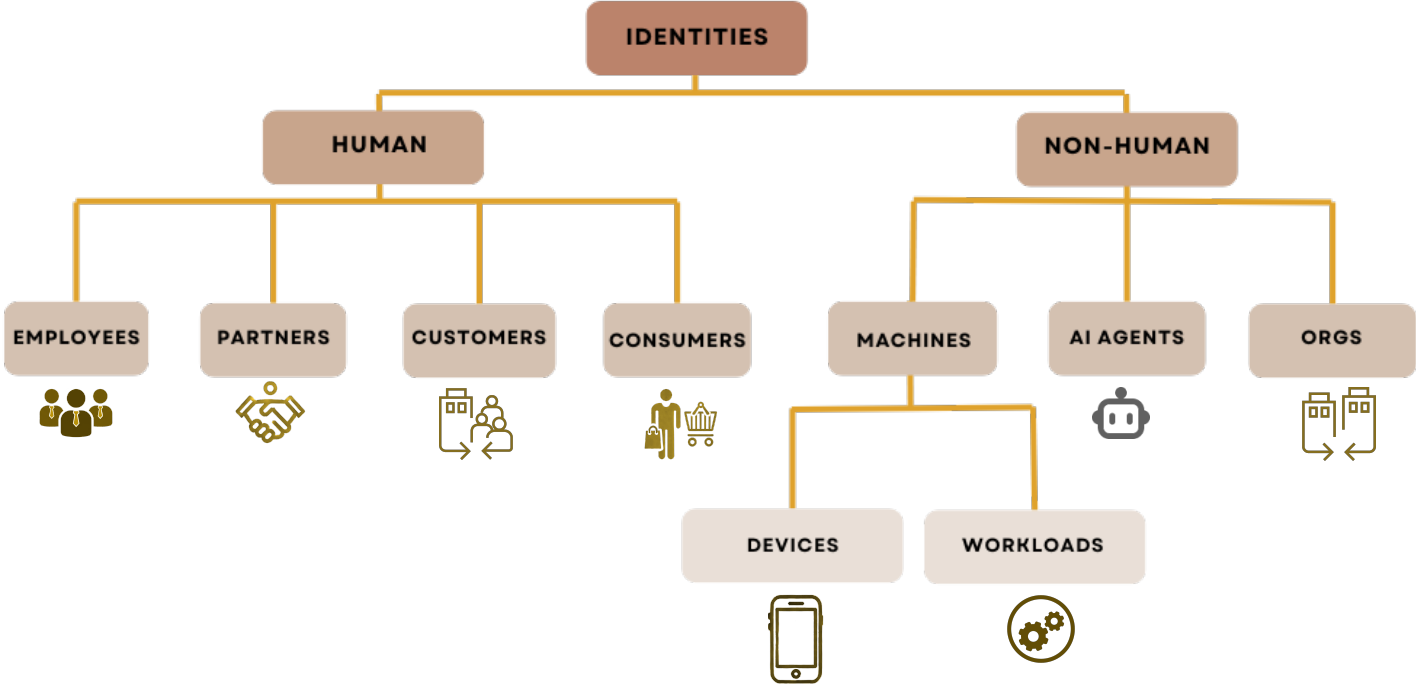
Sources: [Gartner Press Release](#).



# Identity Explosion Meets Cloud + AI

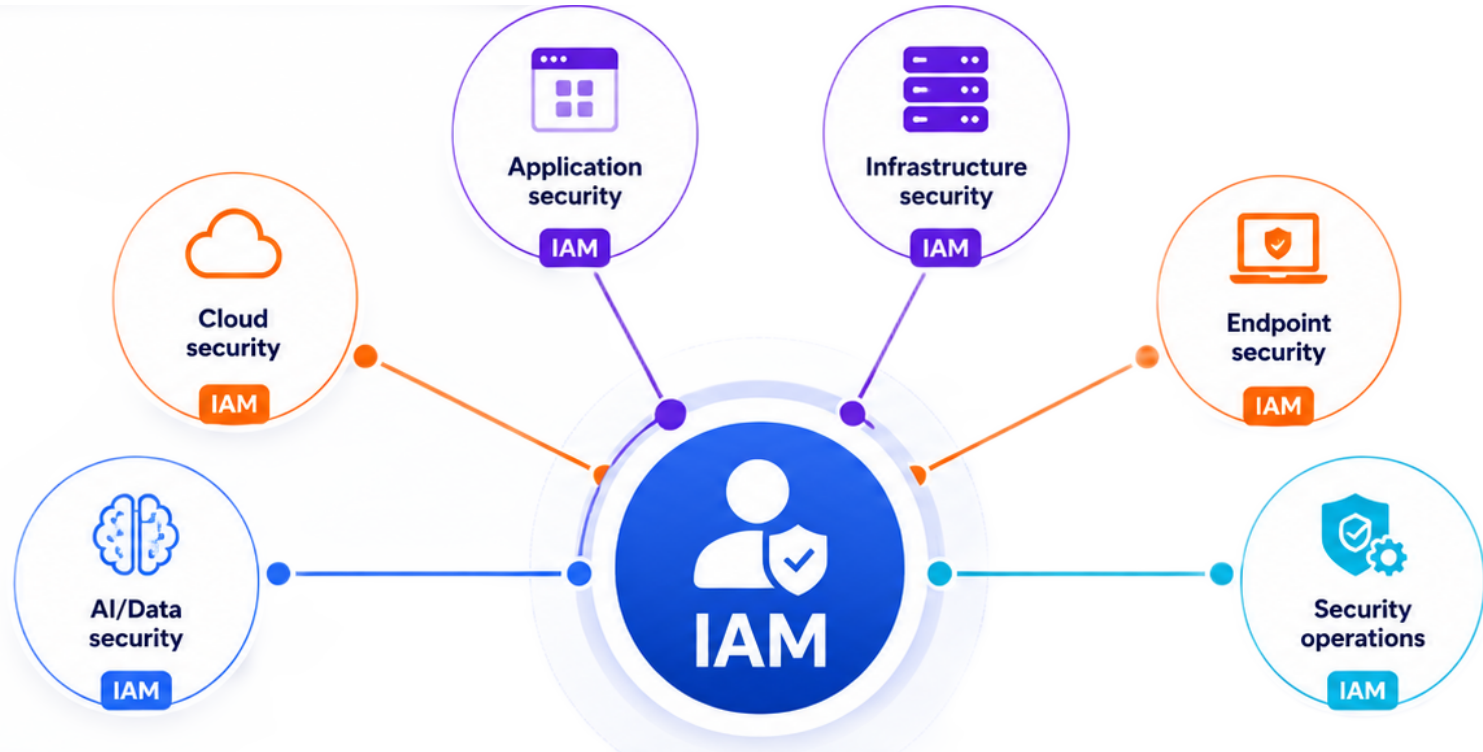


# Agent ID is seen as an Evolution of Machine IDs

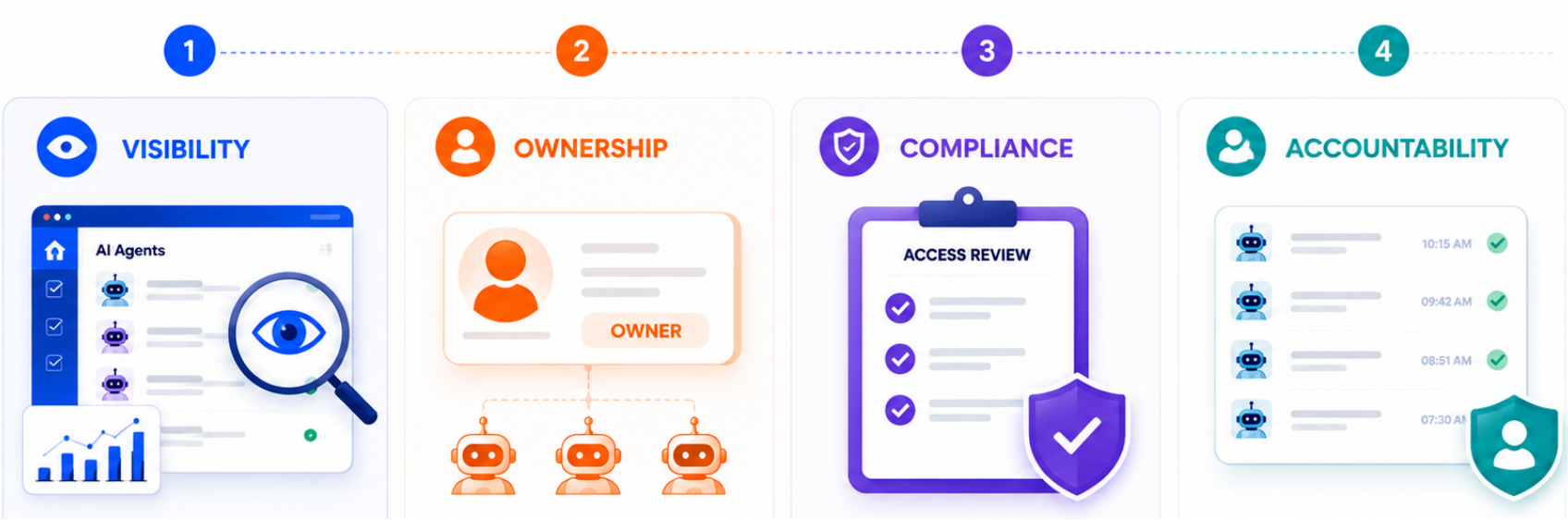


# Identity-first Security

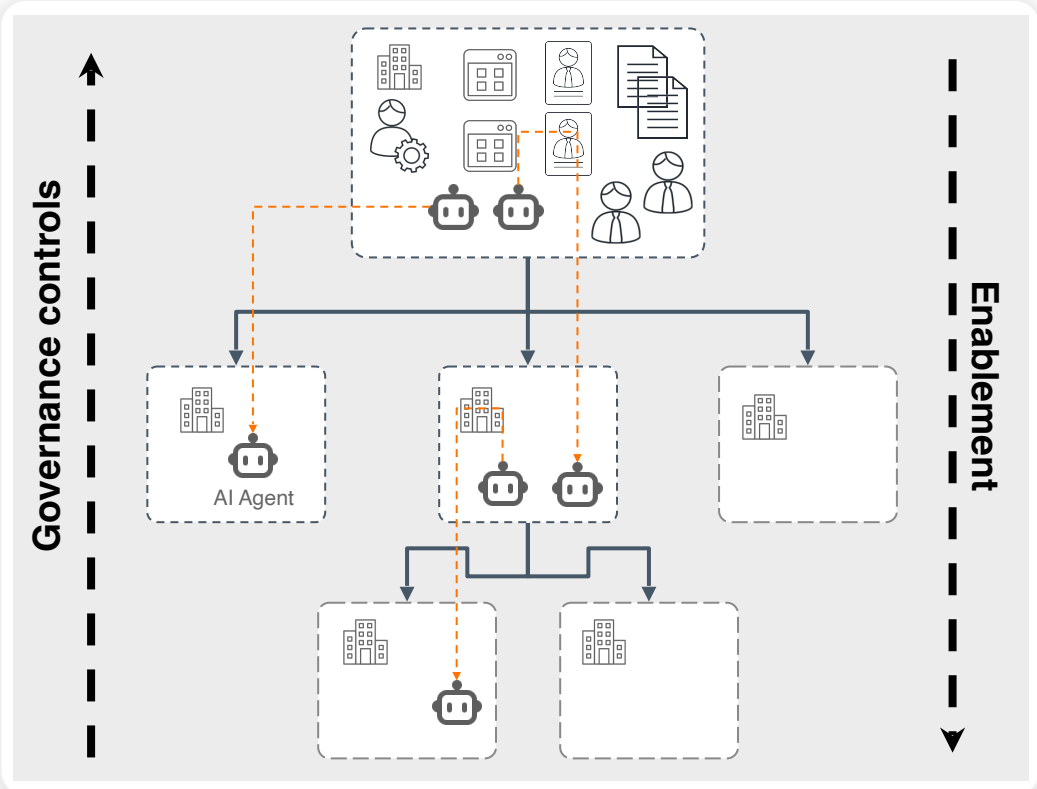
---



# Governance for AI Agents



# Delegated Administration for Agent IDs



# Agentic IAM Protocols

---

- On-behalf-of (OBO) Flow
- MCP
- A2A
- Dynamic client registration
- ABAC, ReBAC and RAR
- CIBA
- Workload federation and token exchange
- Secure Vault



# Other Emerging Protocols

---



Internet of Agents



Agent Network Protocol



AI Agent Protocol



Trusted Commerce Protocol



Agentic Commerce Protocol



A URI-Based Framework  
for Interoperable Agents



NANDA Project



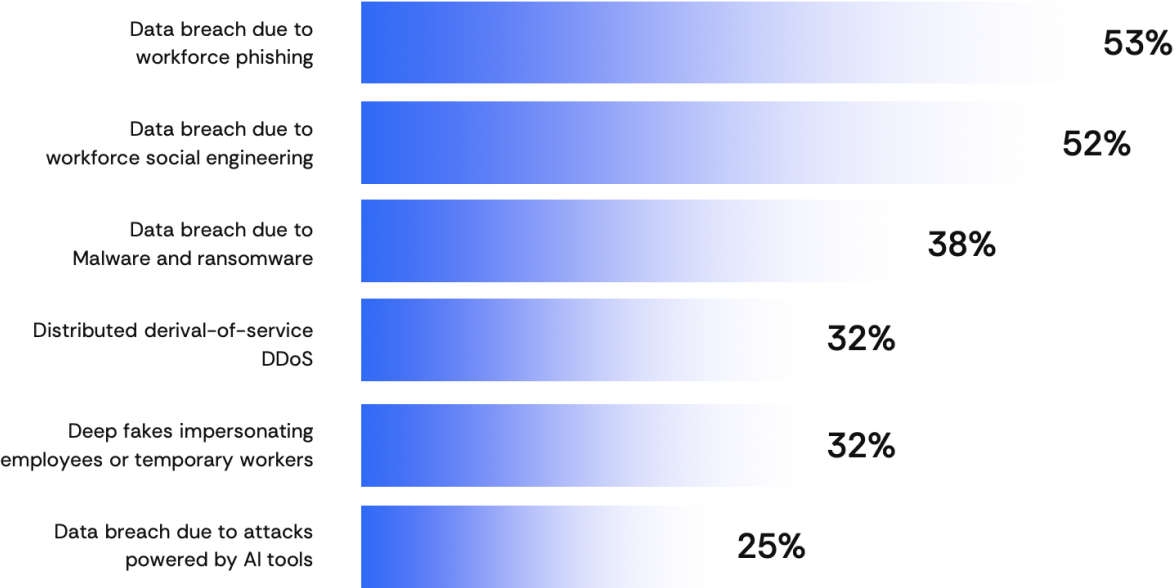
Agent Payments Protocol



# AI vs IAM

# Deep fakes and AI powered attacks are growing concerns

---

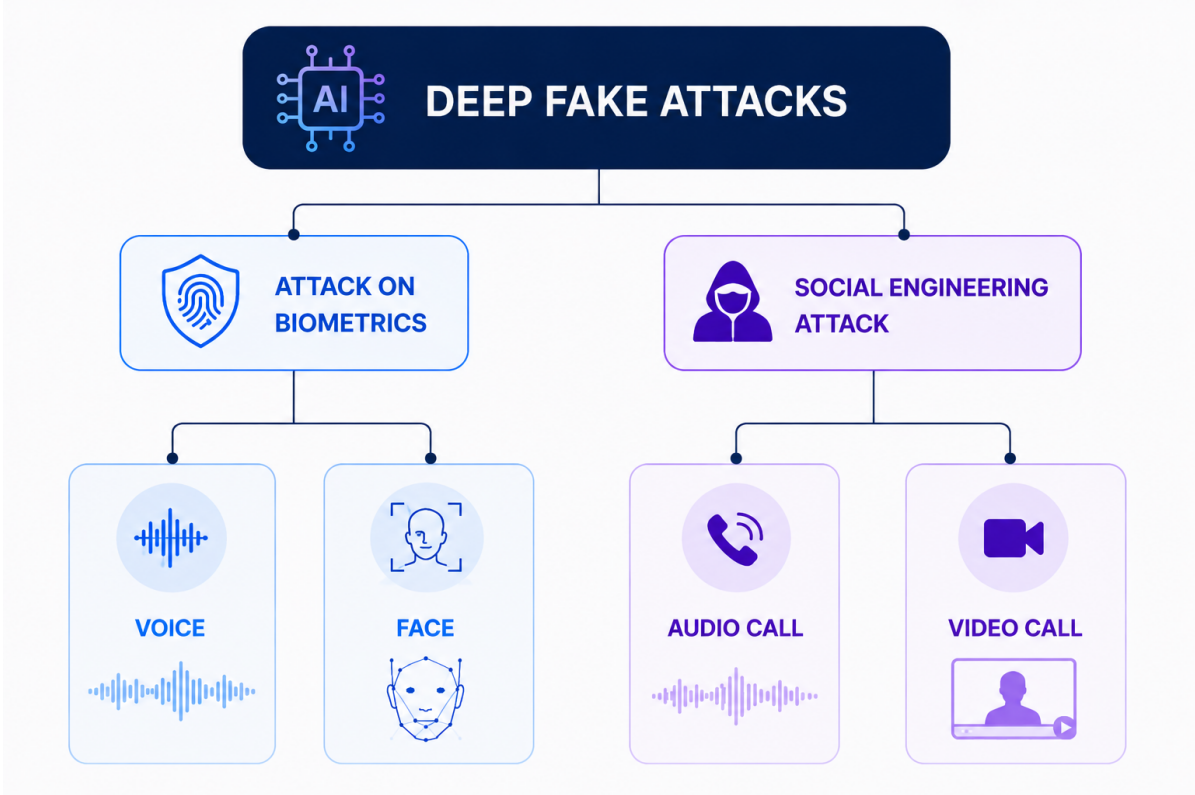


Source: Datos Insights – Financial Crime and Cybersecurity Forum

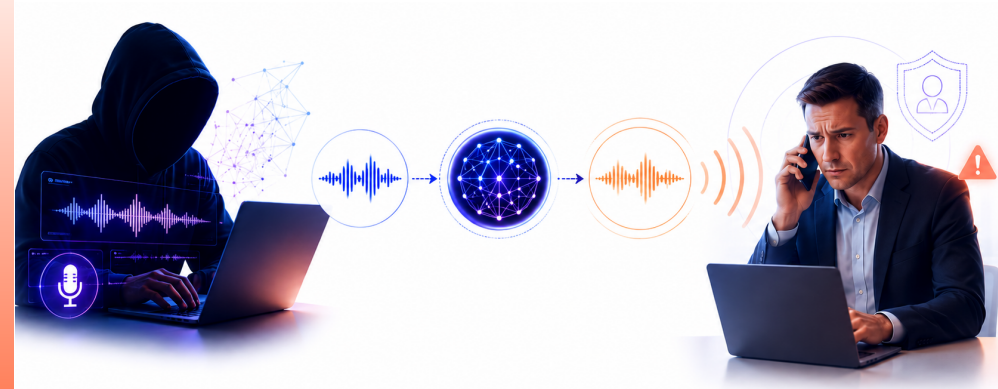


# Deep Fake Attacks

---



# Deep Fake Voice Detection



ElevenLabs

Get started free

## Clone your voice in every language, in minutes

Upload a short recording and get a voice clone that sounds just like you. Produce ads, videos, podcasts, audiobooks, and more in 70+ languages with zero production time.

Clone your voice free

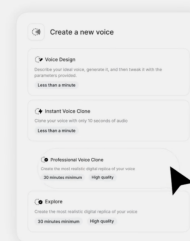
- No credit card required
- Join 7,500,000+ teams and creators
- Cancel anytime



Voice cloning saves me considerable time and cuts down on costs associated with traditional voice actors. Incredibly useful, especially in creating voiceovers for my TikTok and Instagram videos.



★★★★★  
Chester M. • Verified G2 review



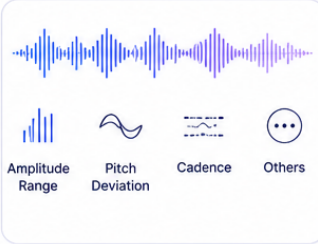
See it in action



# Deep Fake Voice Detection



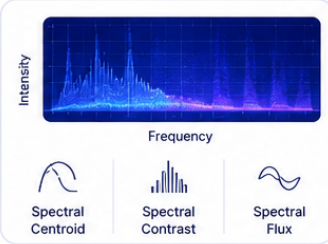
## ANALYSIS OF PERCEPTUAL FEATURES



Signal processing analysis of amplitude range, pitch deviation, cadence and others.



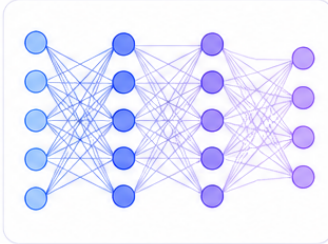
## SPECTRAL FEATURE-BASED DETECTION



ML-based analysis of features such as spectral centroid, contrast and flux.



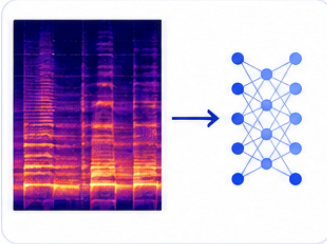
## DEEP NEURAL NETWORK



Training on huge datasets to allow the DNNs to learn and identify artefacts used for inference/classification.



## MACHINE VISION



Translation of audio spectrograms into images which are then classified using vision-based ML or DNN models.



# Multi-layered Defense for Voice

---

- Caller ID Spoofing
- IMEI Spoofing
- Sim Swap detection
- Phone/identity correlation services



# Face Deep Fakes

- **Presentation attacks**

Fraudulent artifact is presented to the physical sensor (camera).

- **Injection attack**


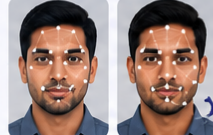



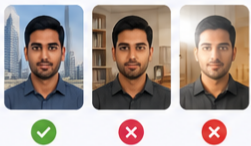
Digital content is introduced into the IDV process by-passing the physical sensor (camera).



# Deepfake Face Detection

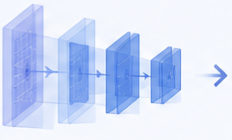

## 1 IMAGE FEATURES

Analyzes visual cues and inconsistencies present in the face and surrounding context.

-  Facial landmark alignment and mobility  

-  Blink analysis  

-  Inconsistent or repeated backgrounds / clothing / glare / shadows  


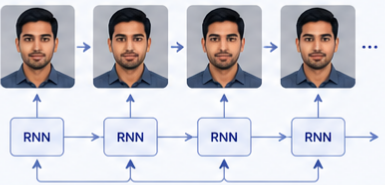
## 2 NEURAL NETWORKS

Deep learning models learn complex patterns and temporal relationships.

 → 

**CNNs**  
Detect pixel-level anomalies

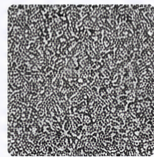
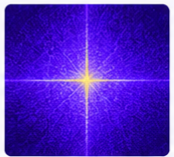
---



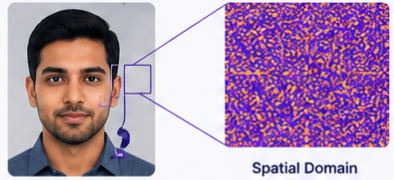
**RNNs**  
Detect temporal inconsistencies between frames

## 3 GAN / DIFFUSION FINGERPRINT DETECTION


Identifies subtle traces left by generative models in both frequency and spatial domains.

 → 

Generated Face → Frequency Domain (Noise Pattern)



Spatial Domain (Micro-patterns)

 Detects invisible fingerprints and artifacts that are difficult for the human eye to see.



# Multi-layered Defense for Face



# Social Engineering against Employees









AI DEFENSE BOT MONITORS THE CALL



# AI for IAM

# GenAI Fit for Purpose

---

Criteria	Fit for GenAI
Can be done well (enough) by humans	 Yes
Priority is acceleration	 Yes
Requires clear human accountability	 Somewhat
Priority is quality	 Somewhat
Requires real-time or near real-time responsiveness	 No
Requires deterministic decisions	 No





# Where GenAI is not fit for purpose

---



## Authentication



---

-  Requires high performance
-  Must be a deterministic decision



## Authorization

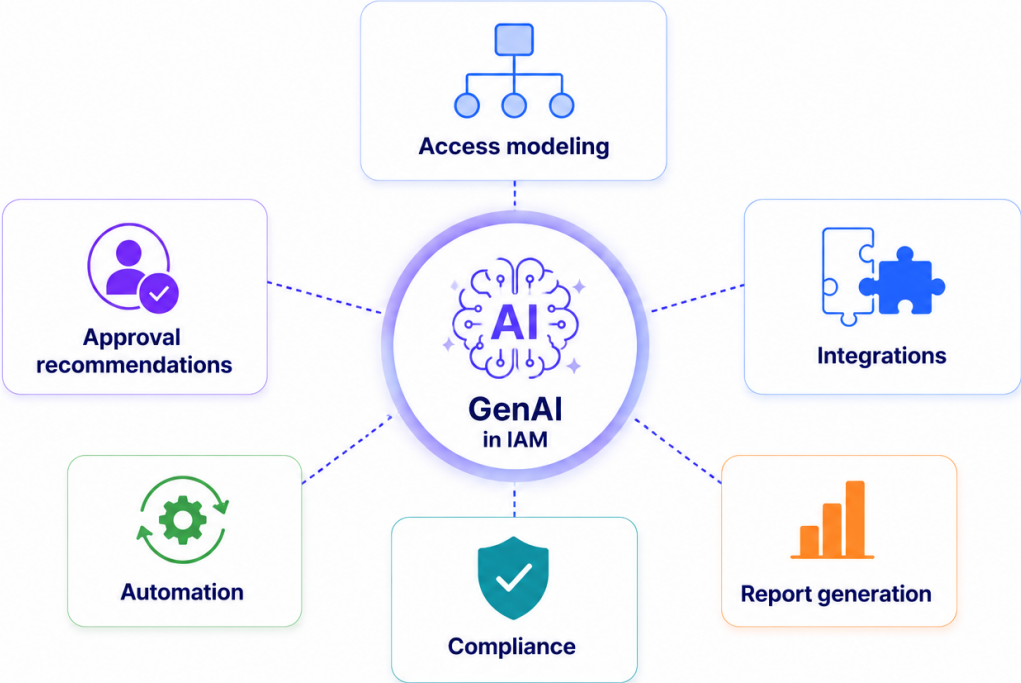
---

-  Requires high performance
-  Must be a deterministic decision



# GenAI Use Cases in IAM

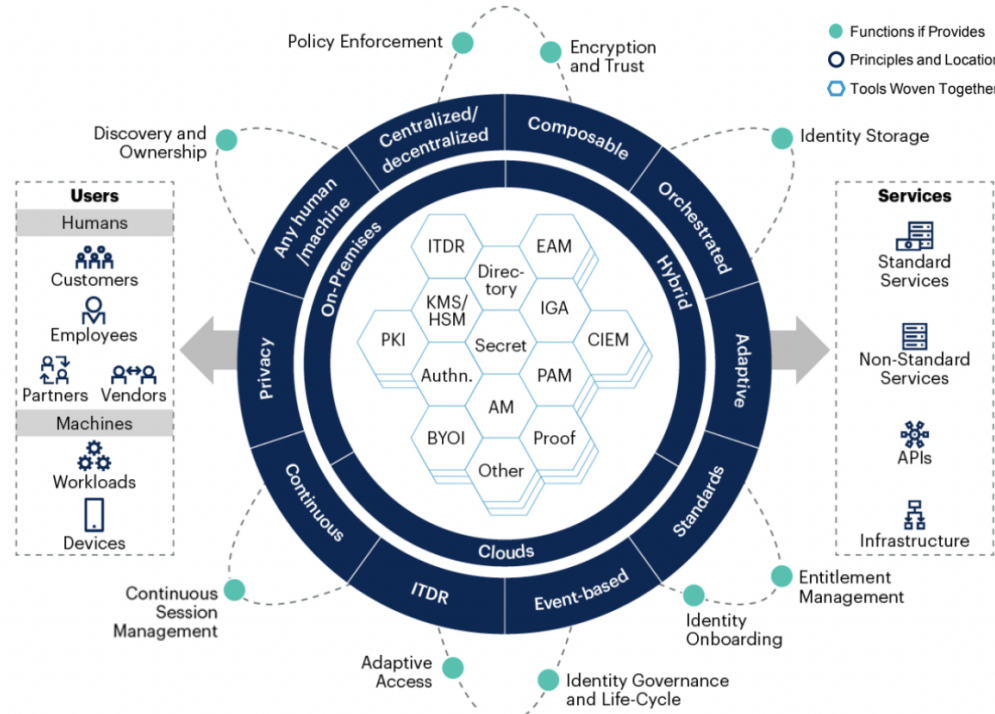
---



# Machine Learning for Continuous Risk-based Authentication



# The Identity Fabric



\*Source: Identity Fabric - The Definition and its Architecture - Felix Gaehtgens, Gartner IAM Summit 2024, London





AI is not just another technology cycle; it is a paradigm shift underway.

And IAM is being completely reconstructed.





May 20 - 22, 2026 | Austin, Texas, USA

# Thank You!



**Johann Nallathamby**

Senior Enterprise Architect & Field CTO

