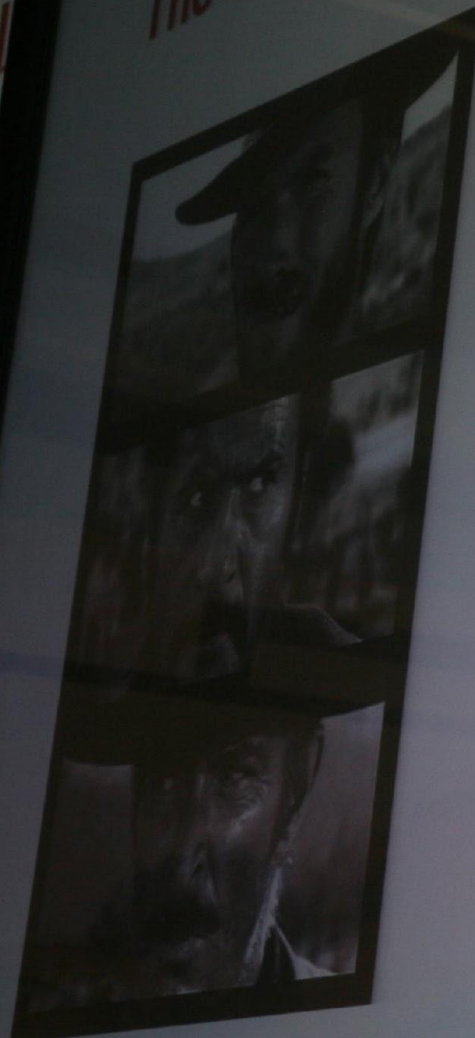


---

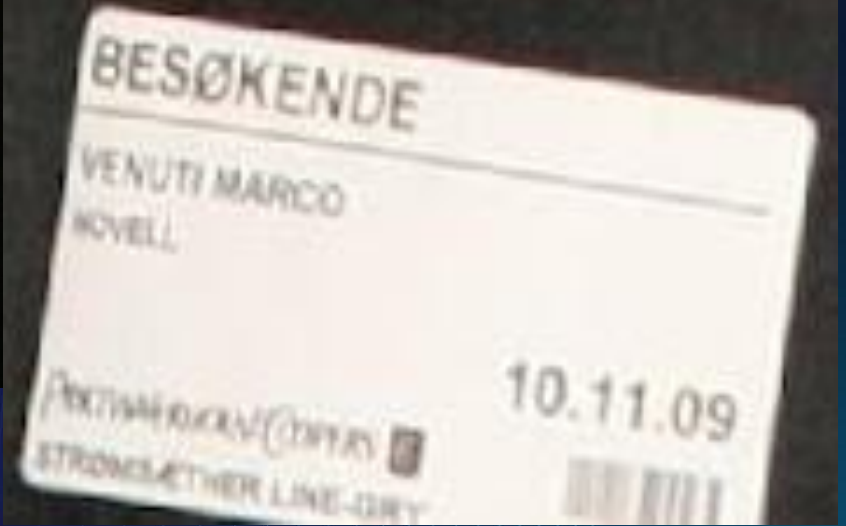
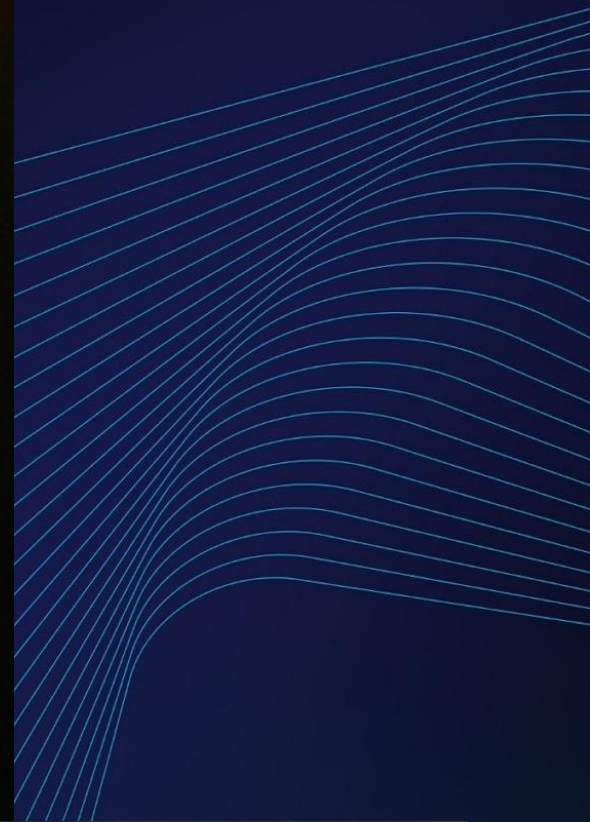
**Identity**  
**Day**

N

# The Good the Bad



Country	International release date	Date
Italy		December 15, 1966
United States		December 23, 1967
Germany		December 29, 1967
Japan		December 30, 1967
Finland		February 2, 1968
France		March 8, 1968
Denmark		April 8, 1968
Sweden		April 10, 1968
China		June 13, 1968
United Kingdom		August 22, 1968
Pakistan		July 21, 1974
Philippines		August 7, 1977
Norway		October 8, 1982



# The Good, the Bad and the Ugly



International release dates	
Country	Date
 Italy	December 15, 1966
 United States	December 23, 1967
 Germany	December 29, 1967
 Japan	December 30, 1967
 Finland	February 2, 1968
 France	March 8, 1968
 Denmark	April 8, 1968
 Sweden	April 10, 1968
 China	June 13, 1968
 United Kingdom	August 22, 1968
 Pakistan	July 21, 1974
 Philippines	August 7, 1977
 Norway	October 8, 1982

# IAM 2026 - The Good, the Bad and the Ugly

Good



The average enterprise manages 370+ applications – **40% don't support modern identity standards...yet**

Bad



**Siloed IGA, PAM, AM** solutions create inconsistent policy enforcement & visibility gaps

Ugly



Traditional IAM is *designed for humans* – **Not for AI agents** operating at machine speed

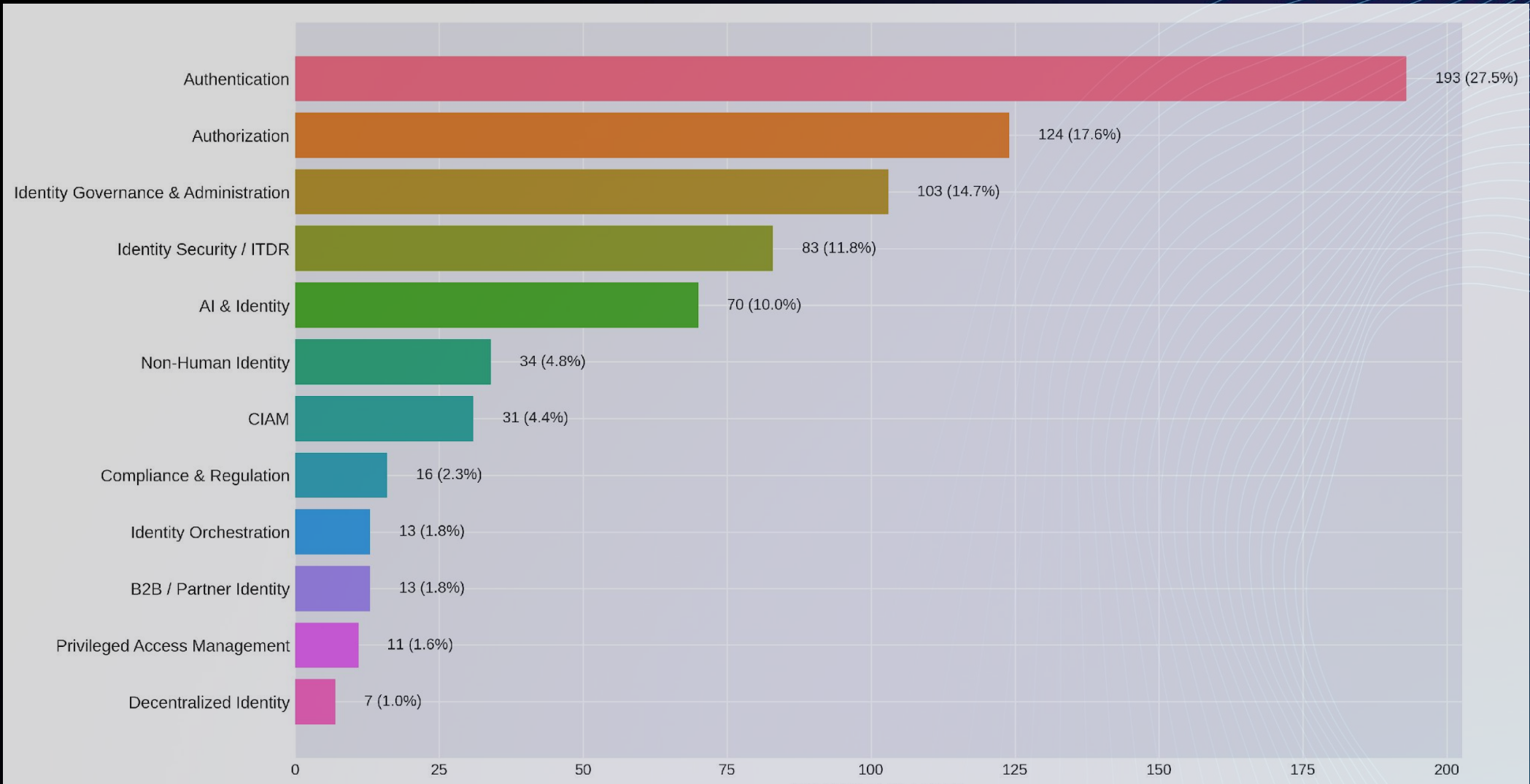
# When Identity Works, But Not Together

*Addressing the IAM Fragmentation*

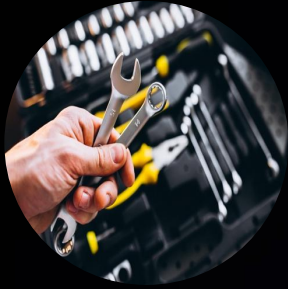
Marco Venuti  
Thales

# Major IAM conference in US

## Submission count per IAM solution domain



# Adoption pattern - Reality check



## Best of Breed

### Mature capability

- ❑ Specialized IAM solutions from multiple vendors
- ❑ Fragmented / heavy reliance on integrations



## Reality

### Eventual State

- ❑ No organization is IAM greenfield
- ❑ No IAM vendor excels in every capability



## Converged Suite

### Easy Procurement

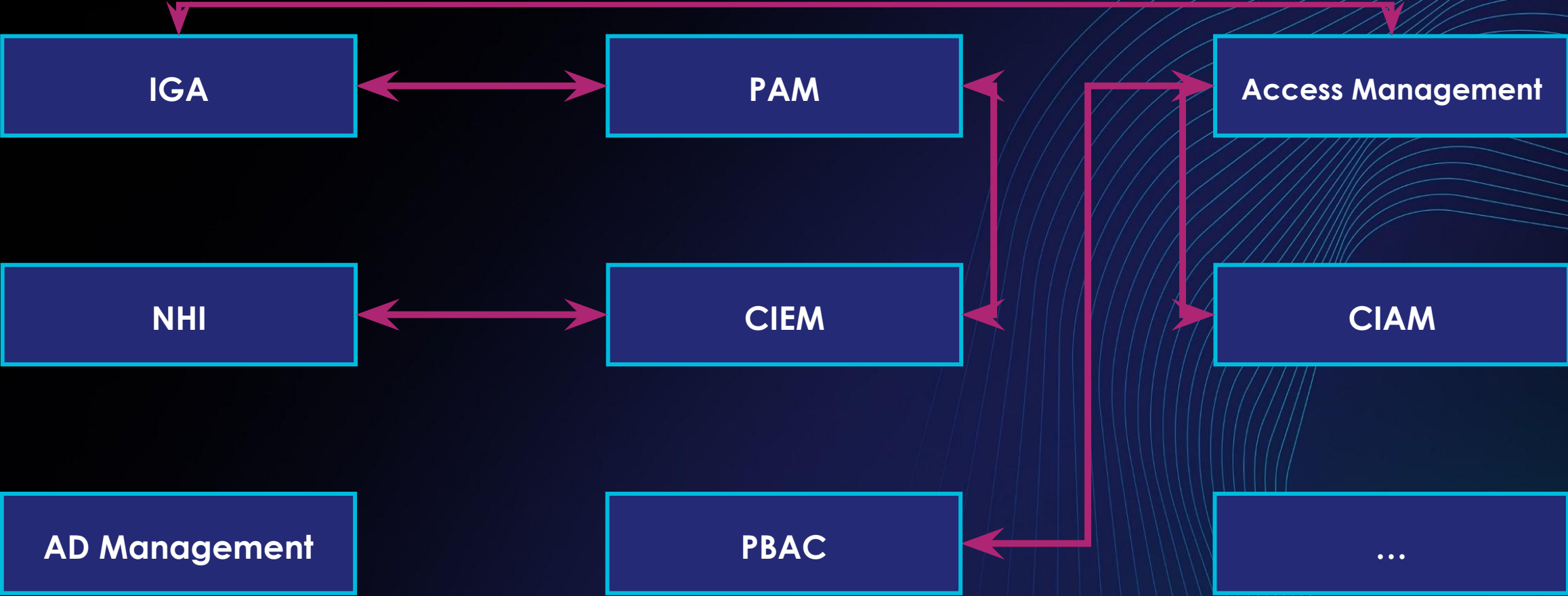
- ❑ Reduced number of vendors covering multiple IAM capabilities
- ❑ Lower maturity and vendor lock-in

# Too many conflicting objectives

You can only spin 2



# Identity in action – Current state



# IAM adoption assessment

## Identity Works

Vendor provides **GREAT** Identity components

- Capability maturity is not the bottleneck anymore

## But don't cooperate well

The challenge is **COORDINATION**

- Integration layers become the real "identity engine"

*Fragmented security posture*  
*Sub-optimal user experience*  
*Operational complexity*

# The attention shift

**Tools**

*Siloed Capabilities*



**Architecture**

*Coherent Ecosystem*

# Identity Fabric - Definition

The Gartner logo is displayed in a white rounded rectangular box. The word "Gartner" is written in a bold, dark blue sans-serif font.

## **Evolution of IAM infrastructure: from siloed tools to a connected system-of-systems**

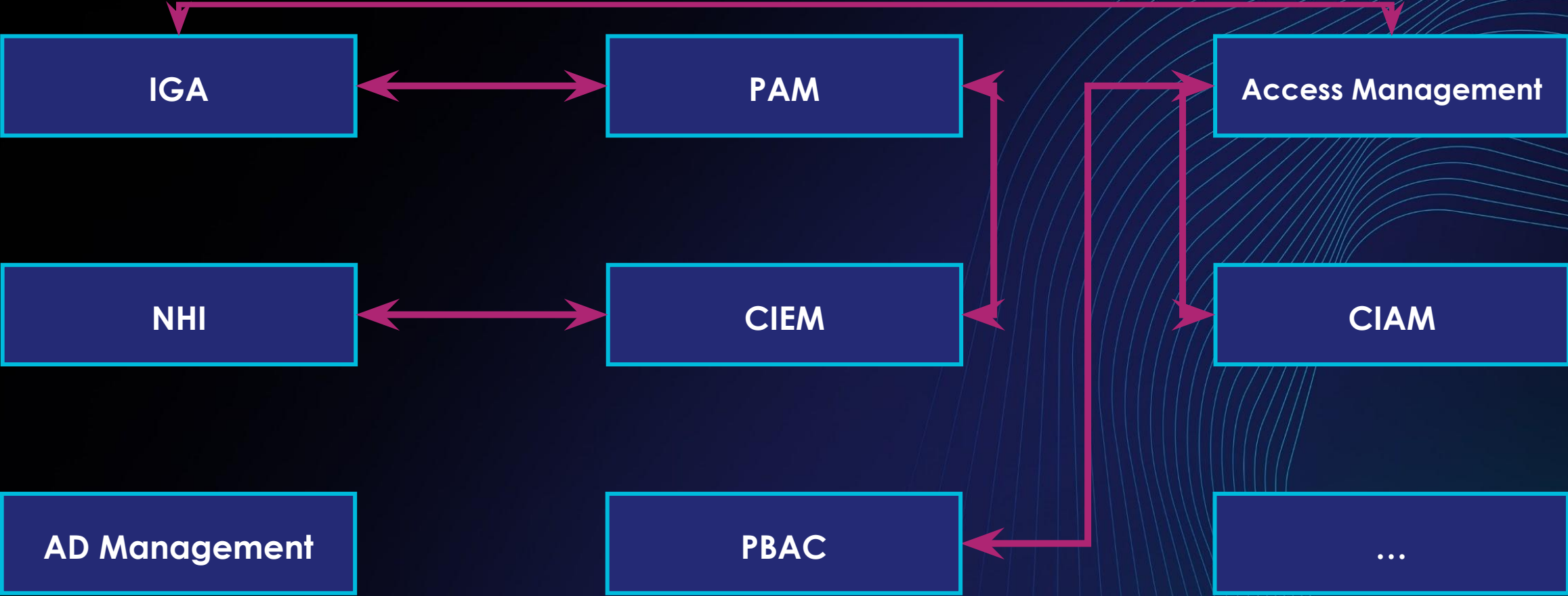
*Strategic evolution of IAM into a connected, risk-aware system of systems designed to support identity-first security for humans & machines*

The Kuppingercoile ANALYSTS logo is displayed in a white rounded rectangular box. The word "Kuppingercoile" is in a bold, dark blue sans-serif font, and "ANALYSTS" is in a smaller, red sans-serif font below it.

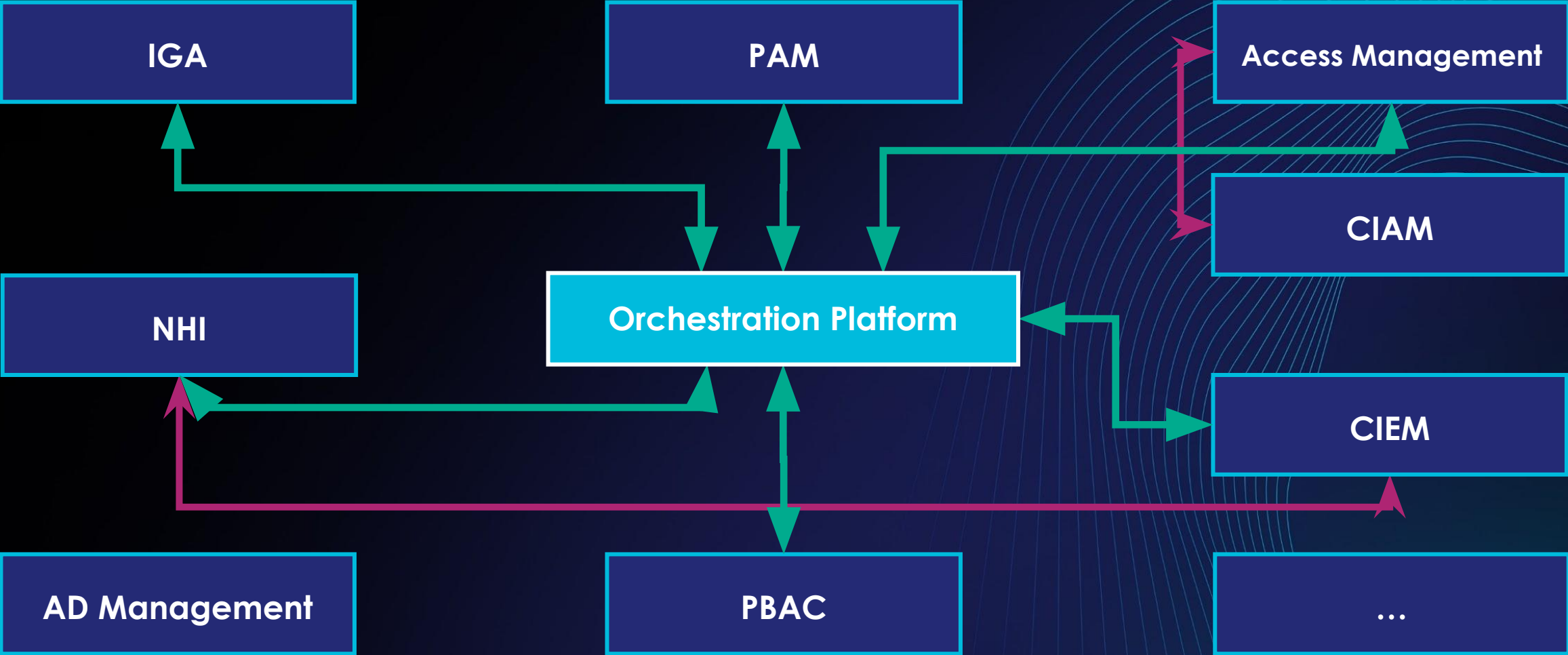
## **An architectural model, not a single product**

*Integrated identity services that delivers seamless, controlled access for all identity types, built from multiple tools, orchestrated as a cohesive "fabric"*

# Identity Fabric in action – Current state



# Identity Fabric in action – Evolutionary state



# Where do you belong?

KuppingerCole poll · Aug 2025 · ~80 IAM practitioners

- Loosely coupled / uncoupled IAM tools
- Converged IAM Suite
- Orchestration of multiple solutions

# Where do you belong?

KuppingerCole poll · Aug 2025 · ~80 IAM practitioners

28%

Loosely coupled / uncoupled IAM tools

33%

Converged IAM Suite

38%

Orchestration of multiple solutions

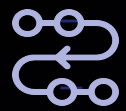
*Majority of organizations are still in traditional IAM architectures*

# Identity Orchestration

## Not just user journey

*[Generalized, stand alone low-code designer and runtime engine for process modeling and interaction management; hybrid deployment friendly]*

### User Journey Modeling



UI and back-end interactions management

Maintain the user journey to flexibly balance usability and security

---

### API level integrations coordination



Streamlined third-party solution interoperability

Scheduled or on-demand event brokering and dispatch

---

### Process & Policies Modeling



JML or other policies modelling and enforcement

Directly in the pipe or relaying on PBAC solutions

**e.g. Improving  
account recovery**



## Onboarding

*Account creation with identity verification*



Attributes Collection



Document Scan



Selfie Match



Passkey Delivery



## Authentication

*Secure and passwordless login experience*



Account Lookup



Credential Check



Access Granted



## Recovery

*Challenge on what you know*



Account Lookup



Security Question  
Email OTP



New Paskey

*“Recovery should prove that you are still the one”*



## Onboarding

Account creation with identity verification



Attributes Collection



Document Scan



Selfie Match



Passkey Delivery



## Authentication

Secure and passwordless login experience



Account Lookup



Credential Check



Access Granted



## Recovery

Recovery through Identity verification



Account Lookup



Document Scan



Selfie Match

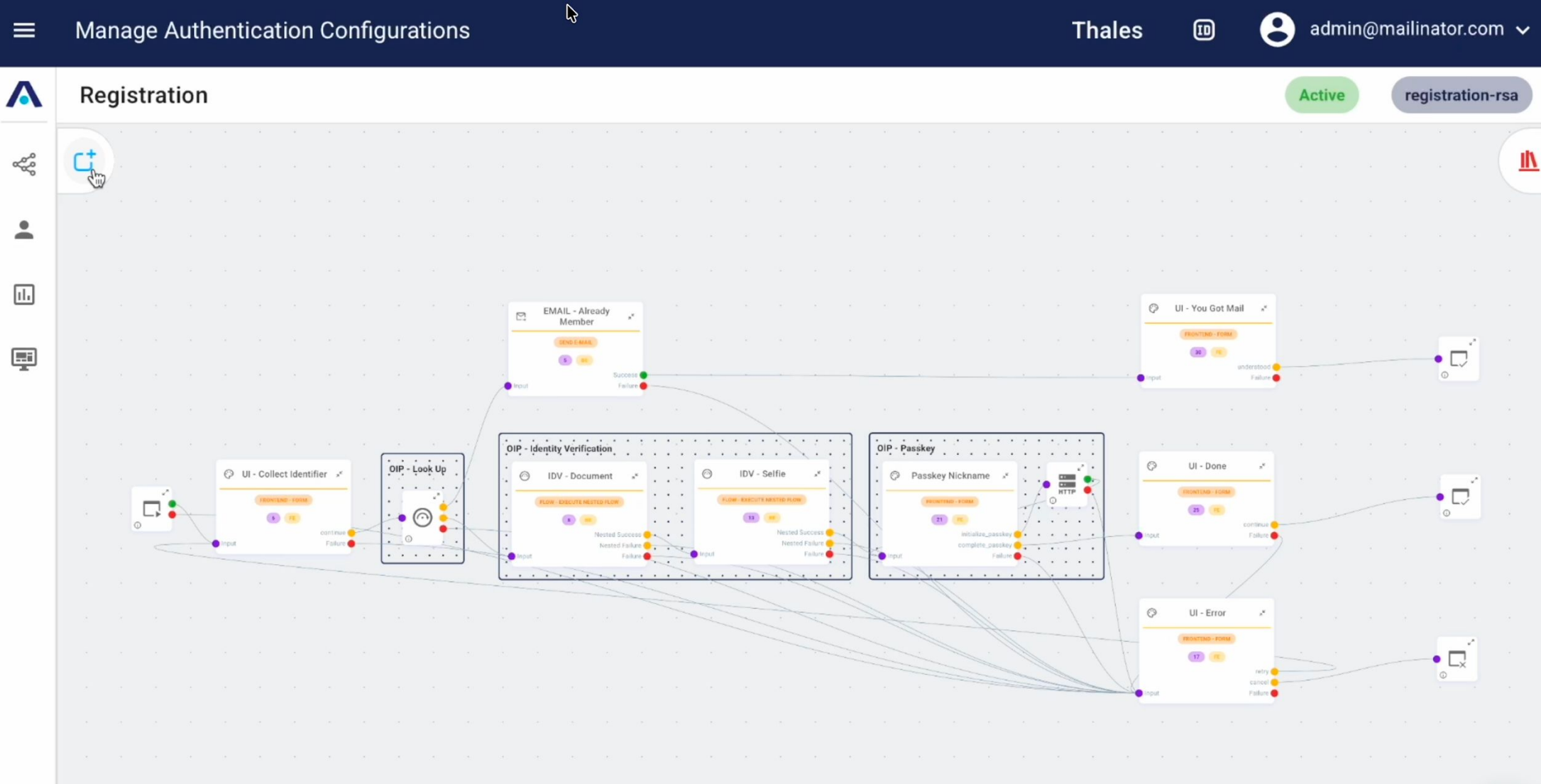


New Paskey

“Recovery can be strong only if Onboarding is Strong”

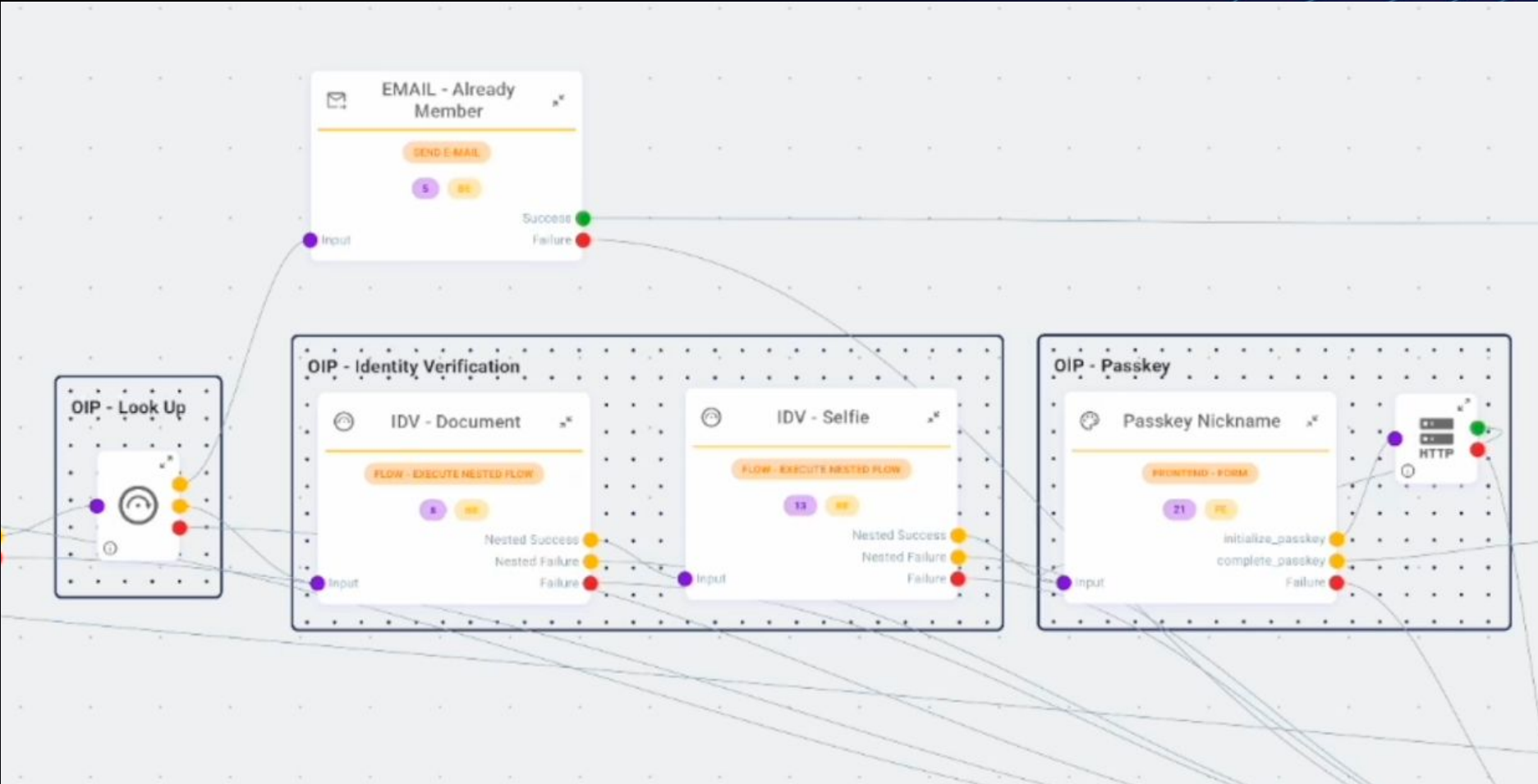
# Identity Orchestration

## Sample Registration Flow



# Identity Orchestration

## Sample Registration Flow



# Welcome

Enter your email address to get started!

Email address

✉ john.doe@example.com

Continue

Lost credentials? [Recover account](#)

EN

Secure Access  
Zero Passwords

Tue 9 Jan

09:41





## Onboarding

Account creation with identity verification



Attributes Collection



Document Scan



Selfie Match



Passkey Delivery



## Authentication

Secure and passwordless login experience



Account Lookup



Credential Check



Access Granted



## Recovery

Recovery through Identity verification



Account Lookup



Document Scan



Selfie Match



New Paskey

“Recovery can be strong only if Onboarding is Strong”



## Onboarding

Account creation with identity verification and BioKey Generation



Attributes Collection



Document Scan



Selfie Match



Bio-Key Generation



Passkey Delivery

"Strong binding between who you are and the away you look, w/o saving PII"



## Authentication

Secure and passwordless login experience



Account Lookup



Credential Check



Access Granted



## Recovery

Leveraging real identity through facial verification



Account Lookup



Selfie Bio-Key Generation & Match



New Passkey

"Recovery can be strong and Frictionless only if Onboarding is Strong"

# Privacy Preserving Biometrics

## You Are Your Token



SCAN



**Face or finger is scanned  
on your device**

- *On any device: phone, laptop, kiosk, shared workstation*

DERIVE



**Your unique key  
is derived**

- *Keys derived from your biometrics on demand, every time*

VERIFY



**The key proves who  
you are**

- *FIDO2, OIDC, SAML, X.509*

DESTROY



**No secrets left,  
Nothing to breach**

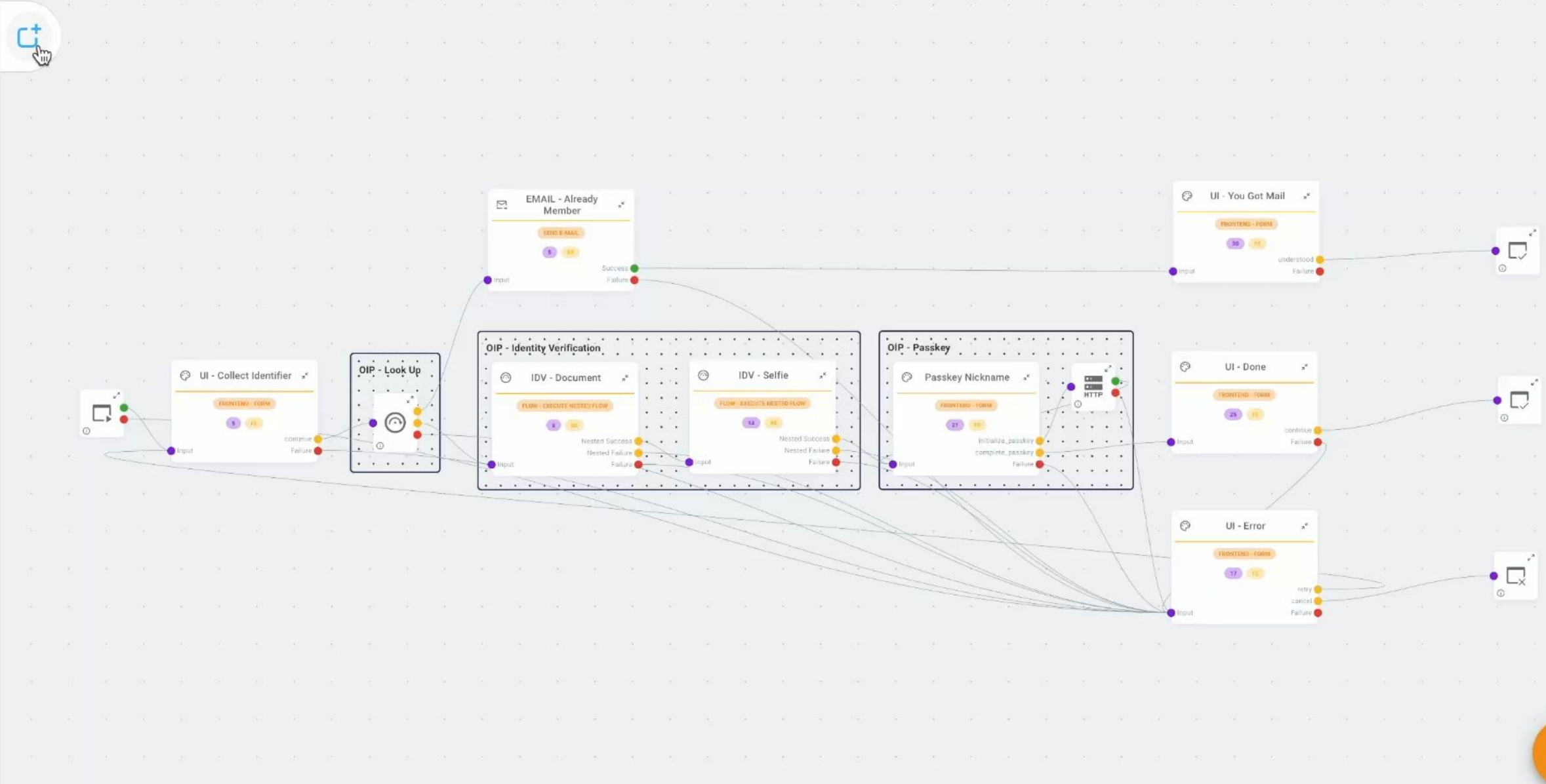
- *Bio scan and private key are immediately deleted*



# Registration

Active

registration-rsa



# Welcome

Enter your email address to get started!

Email address

✉ *john.doe@example.com*

Continue

Lost credentials? [Recover with badge](#)



**Secure Access  
Zero Passwords**



## Onboarding

Account creation with identity verification and BioKey Generation



Attributes Collection



Document Scan



Selfie Match



Bio-Key Generation



Passkey Delivery

"Strong binding between who you are and the away you look, w/o saving PII"



## Authentication

Secure and passwordless login experience



Account Lookup



Credential Check



Access Granted



## Recovery

Leveraging real identity through facial verification



Account Lookup



Selfie Bio-Key Generation & Match



New Passkey

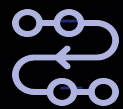
"Recovery can be strong and Frictionless only if Onboarding is Strong"

# Identity Orchestration

## Not just user journey

*[Generalized, stand alone low-code designer and runtime engine for process modeling and interaction management; hybrid deployment friendly]*

### User Journey Modeling



UI and back-end interactions management

Maintain the user journey to flexibly balance usability and security

### API level integrations coordination



Streamlined third-party solution interoperability

Scheduled or on-demand event brokering and dispatch

### Process & Policies Modeling



JML or other policies modelling and enforcement

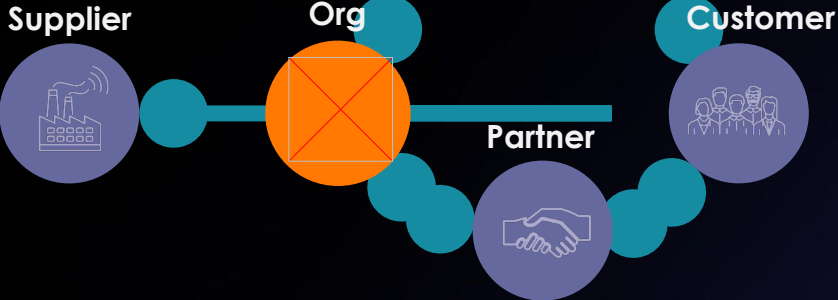
Directly in the pipe or relaying on PBAC solutions

e.g. Improving  
account recovery

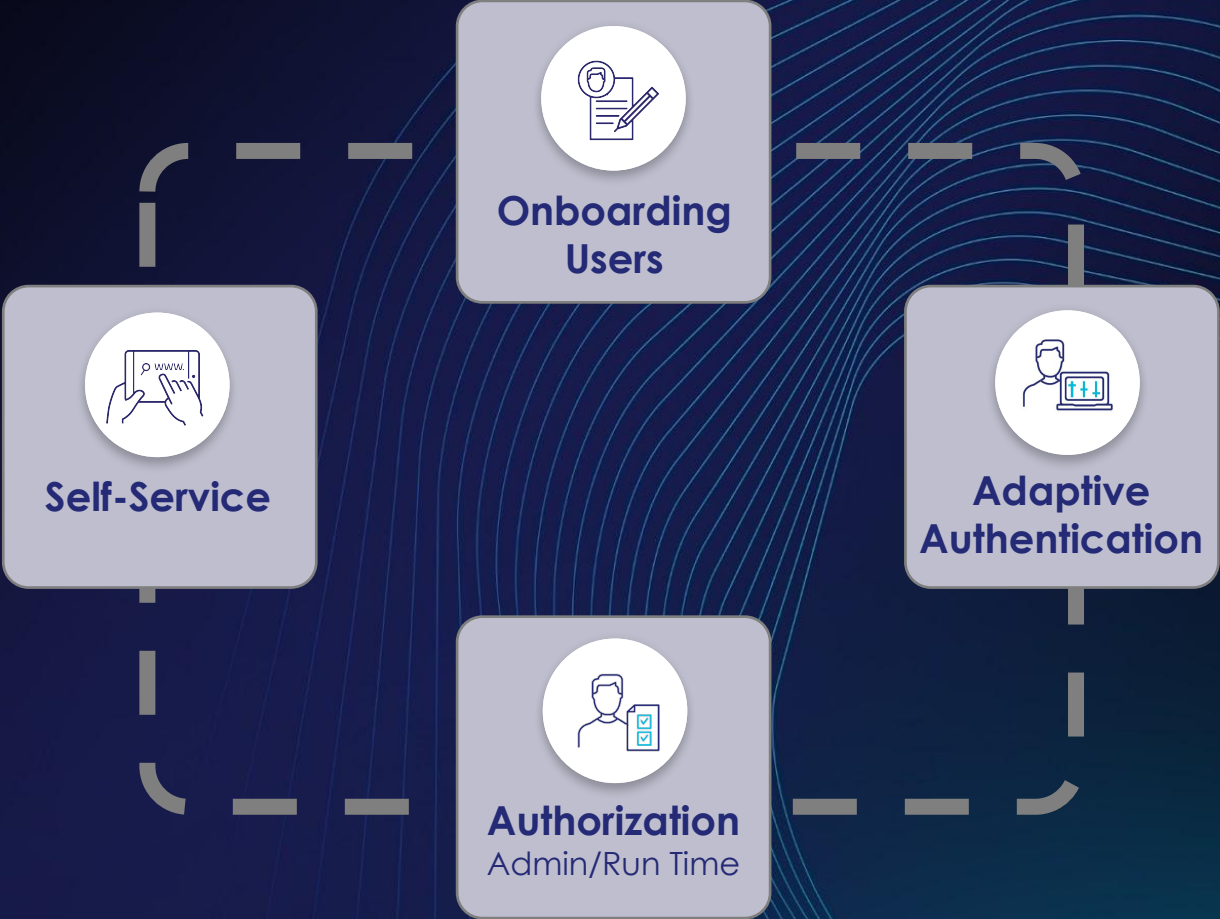
e.g. Addressing B2B-IAM  
requirements

# B2B IAM

## Solution Capabilities



*Traditional B2E or B2C IAM solution fall short in meeting B2B IAM requirements*

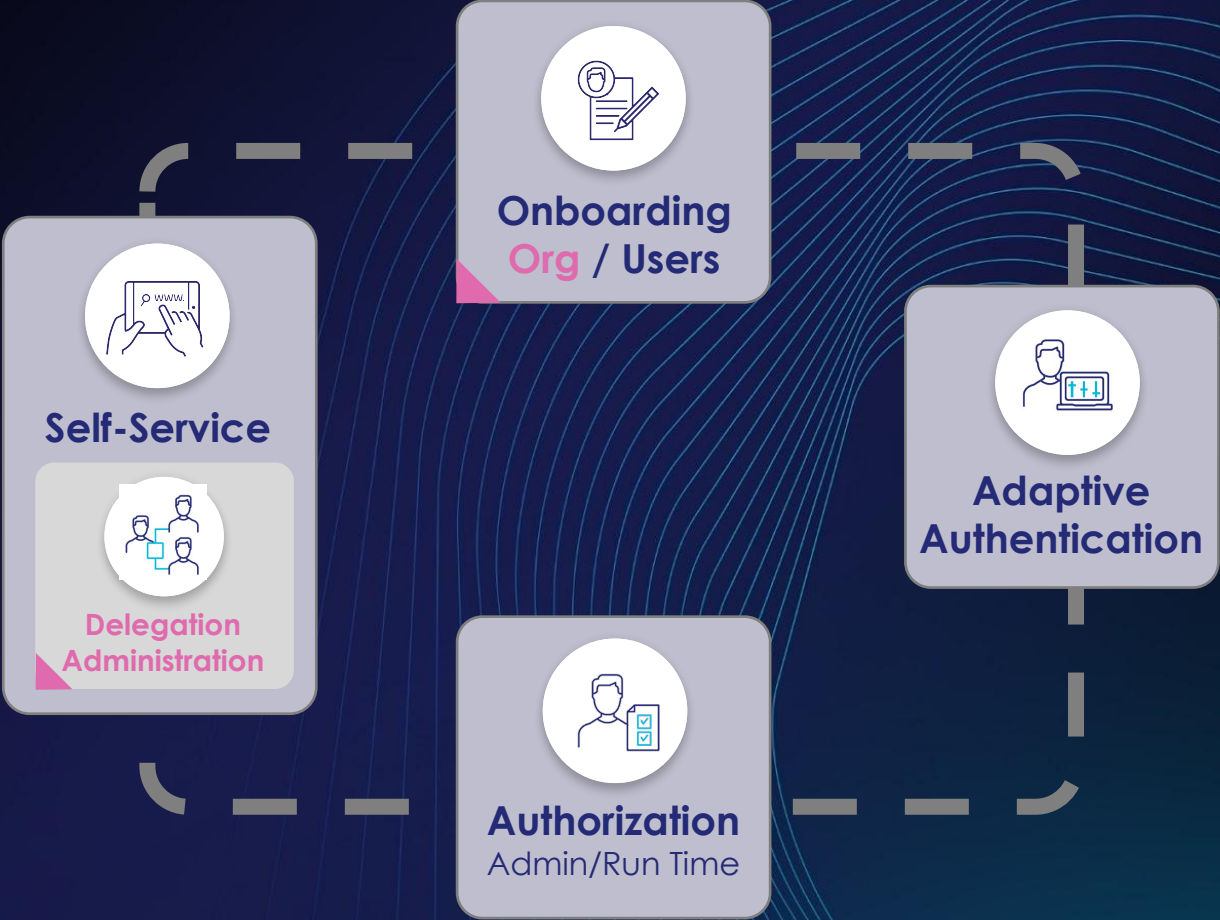


# B2B IAM

## Solution Capabilities



*Specific solutions AND/OR  
integration and extension of in place  
IGA and AM infrastructure*



▲ B2B IAM Specific

# German Creativity, Italian Precision, Danish Clutter

## Subverting Stereotypes in B2B IAM



**Olaf Grewe**

*Head of Digital Identity*

*National Australian Bank*



**Marco Venuti**

*IAM Business Acceleration*

*Thales*



**Jerom Thosterson**

*IAM Architect*

*Salling Group A/S*

# Addressing the IAM Fragmentation

- Fragmented IAM creates security gaps  
***Unification is essential***
- Identity is the #1 attack vector  
***Identity Fabric is becoming a defense measure***



**Orchestration helps but is not sufficient**

Identity Fabric is an architecture paradigm — not just a product

THALES

CYBERSECURITY

# Thank You

---

[linkedin.com/in/mvenuti](https://www.linkedin.com/in/mvenuti)

# Fuzzy Extraction: The Core Innovation

## Deeper dive

Biometrics are inherently noisy; your face or finger scan varies slightly each time....yet there are ways to address that

### **Fuzzy Extraction**

Cryptographic method that reliably derives the same key despite biometrics natural variation

### **The Fuzzy Extractor**

*A pair of algorithms that derive the same cryptographic key from slightly different biometric inputs*

#### ∞ Onboarding Time



User presents an Id (e.g email)



Biometric features extracted



Gen() algorithm produces private key K and public P



P is bound to user profile; K is destroyed

#### 🛡️ Authentication time



User presents an Id (e.g email)



Biometric features re-extracted



Rep() algorithm reconstructs the same K



K signs an AuthN challenge; then destroyed

# What is Identity Fabric?

**A unified architectural framework that orchestrates disparate IAM systems into a single, cohesive control plane.**

Key characteristics:

- Abstraction layer — connects existing IAM tools without rewriting code
- API-centric and microservices-based design
- Vendor-neutral and composable — reduce lock-in
- Identity types agnostic: human, machine, and AI agents
- Enforces consistent policy across cloud, hybrid, and on-prem environments
- Enables Zero Trust as an operational reality, not just a principle

# What to know more?

Manage self-service configurations

Thales  admin@io-demo.com

### Simple Sign-Up

A flow that allows the user to register an account with his email address. The user can give attribute consent (to receive newsletters) and must give document consent.

Active Registration



00:06 / 00:07 1x



Thales IO en



Thales IO sp

# The Problem

Identity-based attacks account for  
**30%** of all intrusions

(IBM X-Force 2025)

**86%** of data breaches involve  
stolen credentials

(Verizon DBIR)