



The State of Identity Security 2026



**Henrique
Teixeira**
SVP Strategy



David Lee
Field CTO

**“ Going into space
battle using Sticks
and Stones ”**



Forces Reshaping Identity Security

Blind spots across human,
machine identities and AI

Economic, regulatory,
and geopolitical
instability

Volatility



Visibility Gap



Disinformation Security



Identity now includes
narrative integrity, not
just authentication

Hybrid Intelligence



Humans and AI agent
co-managing critical
operations

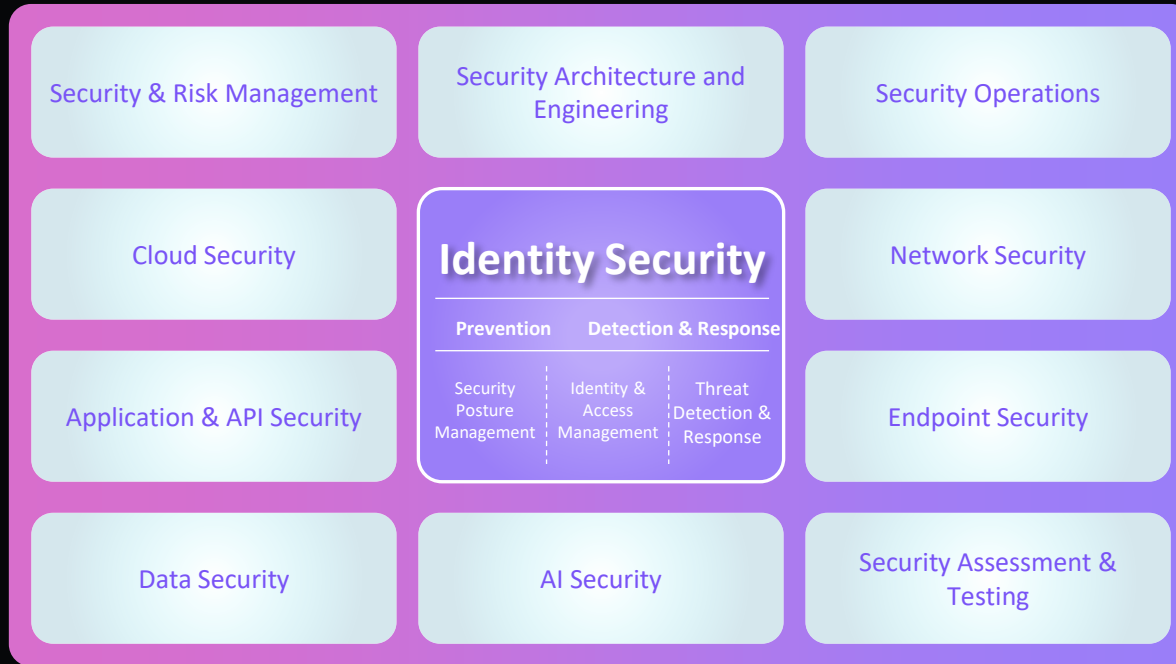
Five forces are rewriting
the rules of security...
and business.

Excitement giving way
to realism on risks

AI Pessimism



Identity is at the Center of Cybersecurity



In the post-cloud, AI-first world, the battlefield is the identity.

The New AI Risk Surface
*From Chaos to
Ruthless Optimization*





The New AI Risk Surface
**AI is not just a tool. It's a
new abstraction layer.**

The Leadership Imperative

Identity security is the operating system for resilience





Top Trends In Identity Security 2026

Identity Security Trends

2026

Platformization
2.0

Rise of MCP

Modern
Machine IAM

Visibility &
Intelligence

AI Governance



Platformization 2.0

What is it

- **Promise: Single Pane of Glass**
- 16+ acquisitions in 2025, \$26+ B
- ~80% of orgs want it

What to do

- **Pause: Is that what you need?**
- Choose a list instead, clusters
- Have business-driven convos

Rise of MCP

What is it

- **The Next REST API Moment**
- Three months almost feel legacy
- 85% of attacks are successful
- OAuth injection affects 43%

What to do

- **Avoid Past Mistakes**
- Move fast, but govern now,
minimum scope
- Use short-lived OAuth 2.1





Modern Machine IAM

What is it

- **SPIFFE/SPIRE, dynamic, ephemeral**
- 70% of secrets in 2022 still active in 2025
- Less than 10% of orgs have a mature NHI strategy

What to do

- **Contain: Avoid building new AI agents, machines with old static keys**
- Start migrating, use SPIFFE
- Manage the remainder aggressively, discover, vault, govern

Visibility and Intelligence

What is it

- **Understanding digital assets**
- ISPM, IVIP
- 80% admit they lack complete visibility into active identity threats

What to do

- **Start with identity data**
- Assess ease/speed of integration
- Automate, analyze





AI Governance

What is it

- **Which AI has access to what**
- 90% working on it
- 62% find it difficult, 28% say challenge is severe

What to do

- **Extend your Identity program to include AI**
- Apply least privilege – to YOUR AI scope
- Oversight, review and validation

Stay Ready

2026

Platformization
2.0

Rise of MCP

Modern
Machine IAM

Visibility &
Intelligence

AI Governance



Recommendations

- Rationalize identity vendor choices within clusters
- Don't replicate API mistakes in MCP
- Contain static machine IDs
- Solve visibility and intelligence with identity data in focus
- Extend your IAM program to include AI agents



Thank You!



HYBRID
IDENTITY
PROTECTION

conf25

