
FROM SEEING TO KNOWING
The Identity Observability Frontier
Tal Herman — Orchid Security
identiverse
#identiverse

The Assumption

We govern access.
So we govern identity.

That's the assumption. This session is about what it costs you.

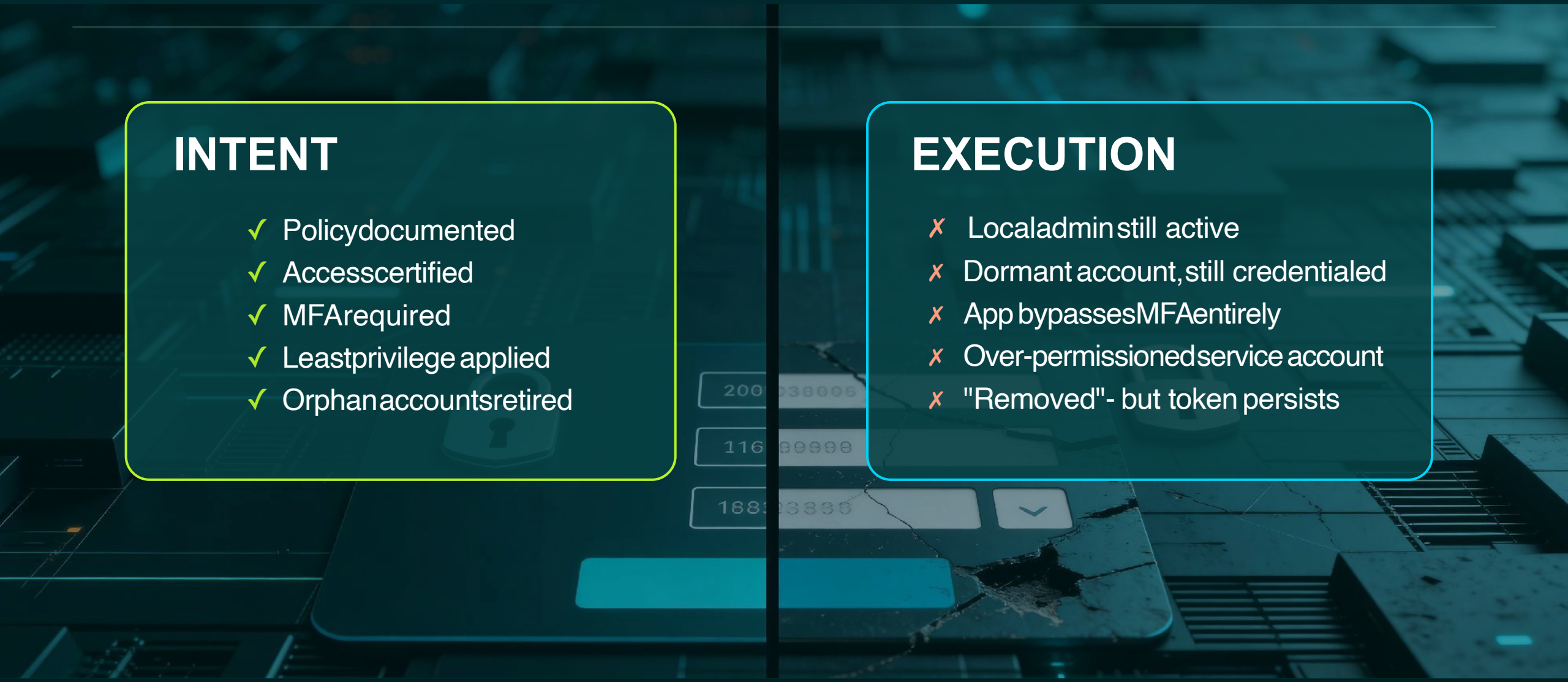
Controversial Take #1

"Your access review is a work of fiction."

Attested. Certified. Signed off.

And still wrong.

Intent vs. Execution



INTENT

- ✓ Policydocumented
- ✓ Accesscertified
- ✓ MFArequired
- ✓ Leastprivilege applied
- ✓ Orphanaccountsretired

EXECUTION

- ✗ Localadmin still active
- ✗ Dormant account, still credentialed
- ✗ App bypassesMFAentirely
- ✗ Over-permissionedservice account
- ✗ "Removed"- but token persists

Identity Dark Matter

60%+

of enterprise identity is **ungoverned** and growing.

Before agentic AI. Before the agent workforce. **This is the baseline.**

> *"The agent executes faster than we can validate. We don't know what access it used, or what it actually did."*

Head of Security, Fortune 500

Agentic Escalation

Agents don't wait for your access review.

80-144×

more machine identities than humans, and climbing

75%

of machine identities have no designated owner.

0ms

the time an agent waits before acting on stale permissions.

Agents Inherit Your Mess...Happily

"AI doesn't create identity problems. It compounds them."

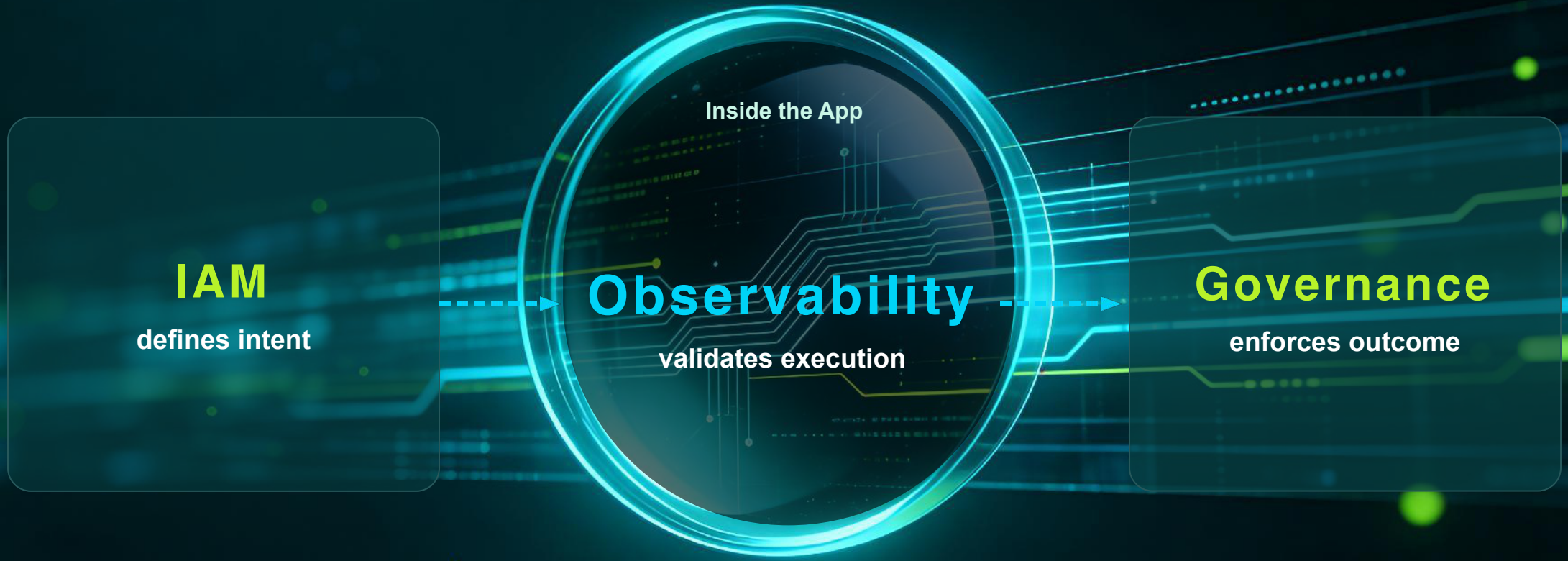
Controversial Take #2

IAM doesn't govern identity.

It governs the pre-defined intention of identity.

And in the agentic era, that distinction <u>will cost you.</u>

Observability is the bridge between intent and execution.



What Observability Looks Like

Who acted

Human, NHI, or agent - attributed and traceable

What they did

Action-level telemetry, not just login events

Should they have

Live policy vs. live behavior - continuously

What happens next

Orchestrated response - not a ticket three days later

Every agent needs an owner.
Every action needs a trace.

Agent

The acting entity requiring ownership.

Tool

The instrument used for the execution.

Action

The specific operation performed.

Target

The endpoint of the trace.

Complete execution traceability at machine speed

Controversial Take #3

Compliance passed.
You're still exposed.

A clean audit proves documentation skill.
Not execution reality.

Compliance Measures Intent
Observability Measures Reality

Compliance asks

- Was access reviewed?
- Was MFA enabled?
- Is there an owner?
- Is policy documented?

Observability asks

- Was it used?
- Was MFA actually enforced?
- Is the owner active?
- Is behavior aligned?

*"Auditors validate evidence. **Attackers validate execution.**"*

So What Does Closing the Gap Actually Require?

OBSERVE

Discover every app/ identity

Human, NHI, and agent.

Surface what they are actually doing inside your applications.

UNDERSTAND

Analyze behavior against intent

Not once a quarter - continuously.

At the moment of execution.

GOVERN

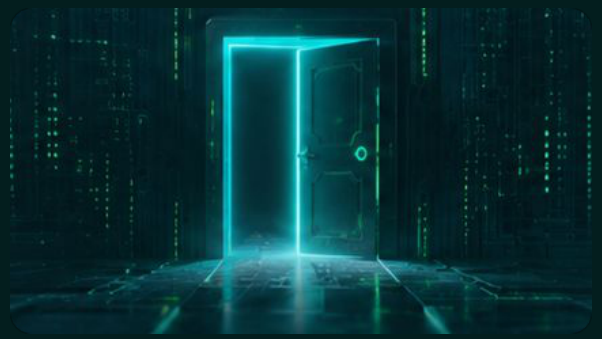
Orchestrate response

Enforce least privilege at execution time.

Attribute every action with full chain of custody.

*"From Identity Dark Matter to **measurable, governed execution.**"*

Stop Governing Intent.
Start Governing Execution.



Visibility

Shows the door.

Observability

Shows what walked through it.

Context

Execution context closes the gap.

tal.h@orchid.security | orchid.security

Meet the team
Booth #239