secours.ai

GOVERNANCE ANALYSIS · JUNE 2026

Machines Don’t Need Identity. They Need a Warrant.

Why non-human identities solve the wrong problem, and why machine governance requires single-use warrants at the execution boundary, not standing permissions.

DOCUMENT

Governance Analysis
NHI vs. Warrant-Based Governance

PUBLISHED

June 4, 2026

AUTHOR

Paul Knowles
Chief Architect, Secours.ai

The Warden Enforcement Plane: deterministic enforcement at the execution boundary, the mechanism this article argues machines need in place of identity.

01

Identity Is the Wrong Instrument

The Cloud Security Alliance recently promoted its NHI Summit 2026 with four learning objectives that reveal, with unusual clarity, where the non-human identity conversation has gone wrong: discovering and inventorying NHIs across complex environments, securing machine-to-machine access, secrets, and tokens, understanding real-world attack paths targeting NHIs, and governing NHIs at scale in AI-driven environments.

Each of these is presumptive. Not wrong in its concern (the operational problems they point to are real) but presumptive in the instrument they assume is the right one to reach for. All four treat the machine's identity as the correct unit of governance. It isn't.

The non-human identity community has correctly diagnosed that machines acting in consequential systems need to be governed. That instinct is right. The implementation fails because it reaches for the wrong instrument.

Credential	An identity instrument. It answers: what is this? It establishes provenance and enables attribution. It belongs in the evidence chain.
Warrant	A governance instrument. It answers: is this specific action sanctioned, by whom, under what conditions, right now? It belongs in the governance chain.

These are categorically different instruments serving categorically different functions. The NHI community has been trying to solve a governance problem by enriching an identity instrument. The result is a credential loaded with authorization scope: pre-signed permission that authorizes classes of action at issuance time and persists until revoked or expired. This is not governance. It is standing permission dressed as a security control.

02

Three Instruments, Three Different Jobs

In a Ward-centric system, the architecture separates three things that current implementations collapse into one.

Identifier	What is acting. Neutral, attributable, traceable. Belongs in the evidence chain. This is what machines genuinely need, and it is the full extent of what they need in terms of identity.
Credential	The identity instrument that verifies the identifier. Currently overloaded with governance weight it was never designed to carry. In a Ward-centric system, the governance function belongs elsewhere by design.
Warrant	The governance instrument that sanctions a specific action against the current interests of a named Ward, at this exact moment of execution. Where accountability is required, it is traceable to a named Principal. Single-use. Exhausted immediately upon execution. Non-transferable, non-inheritable, non-replayable.

The machine carries the identifier. The governance chain produces the Warrant. The credential, as a governance instrument, is unnecessary.

03

The Machine Is Neither

Non-human identity frameworks implicitly treat the machine as a governance object: something that holds authority, accumulates trust, and participates in access decisions. This is the category error in its deepest form. In a Ward-centric system, governance has two anchors, and the machine is neither of them.

The Ward	Authority traces to the Ward as the bearer of consequence: whoever bears the real-world effect of the action, whose payment is processed, whose data is accessed, whose calendar is modified, whose messages are sent. The outer boundary of what any agent may legitimately do is defined entirely by the Ward's current interests, evaluated at the moment of execution. The Ward is not optional.
The Principal	Where accountability is required, it traces to a named Principal who bears liability: the human whose authority made the Warrant valid and who answers for the decision to authorize that specific action at that specific moment. Unlike the Ward, the Principal is optional; where none is named, accountability traces back through the Governance Chain to whoever established the parameters under which the Warrant was validly issued.

The machine requires an identifier to anchor the evidence chain and a Warrant to anchor the governance chain. It requires nothing else.

04

Single-Use, and Exhausted at Execution

This is the property that resolves most of the problems current frameworks struggle with.

A credential that survives execution becomes a liability. It can be replayed against a different target, intercepted and reused, accumulated into a pool of standing permission that grows detached from any original human intent, or silently inherited by downstream agents in a chain. Long-lived tokens and persistent API credentials are among the most exploited attack vectors in enterprise environments for precisely this reason.

A Warrant that exhausts at execution carries none of these risks. The moment the action executes, the Warrant is gone. The next action in the chain requires a fresh Warrant, evaluated against current conditions, bounded by the Ward's current interests. Authority does not accumulate. It does not persist. It does not compound across a chain of agents.

This is the difference between a governance commitment and a structural invariant. The credential model asks the system to honor a policy. The Warrant model makes violation structurally impossible because there is nothing to replay, nothing to inherit, and nothing to intercept that retains any value after execution.

05

Mechanical, Not Discretionary

The objection that immediately arises is implementation. How, in a real system operating at machine speed, does Warrant-based governance work in practice? The answer is that the enforcement plane is purely mechanical. The Warden Enforcement Plane operates at the execution boundary and has no interpretive function, no discretion, and no natural language surface.

Before any agent action produces a real-world effect, the Warden performs a structural check:

- **Does a valid Warrant exist** for this specific action?
- **Is it traceable** to an accountable Governance Chain?
- **Where a Principal is named,** is that Principal traceable and on record?
- **Is it admissible** under the conditions that currently apply?

If yes: mint authority, execute, exhaust, commit to the Exhaustion Registry, issue a Receipt. If no: stop. There is no language model in the enforcement plane, no confirmation prompt, no permission scope, and no token with a validity window. There is a structural invariant at the execution boundary that cannot be circumvented by a sophisticated prompt-injection payload: the payload arrives as a proposed action requiring a valid Warrant, and if no Warrant exists, the action does not execute, regardless of how convincing the payload is.

06

What Three Billion Devices Look Like Without a Warrant Layer

In May 2026, Google announced Gemini Intelligence for Android: a system capable of automating multi-step tasks across apps, processing payments, sending messages, accessing Gmail and calendar, and chaining custom widgets into composed agentic workflows, all initiated by a voice command.

The governance mechanism for all of this is a single confirmation prompt. That confirmation prompt is a credential performing a governance function. It grants admission. It does not govern execution. It authorizes a goal at the point of initiation and then plays no further role in subsequent steps of a chain that may involve payment processing, contact access, and messaging to people who were never part of the original interaction.

At the moment any consequential action is executed, the agent holds standing permission inherited from an instruction issued some time earlier. A prompt injection payload embedded in any content the agent retrieves does not require the agent to manufacture new permissions. It operates within the standing permission already granted.

This is what the credential-as-governance-instrument failure looks like at consumer scale: three billion devices, a confirmation prompt as the only action-time governance mechanism, and standing permission all the way down. Every action in every chain on every one of those devices needs a Warrant: minted for this specific action, for this specific Ward, bounded by the Ward’s current interests, evaluated at the execution boundary, consumed immediately upon execution.

07

The Right Problem. The Wrong Instrument.

This argument is not a case for less governance. The operational hygiene concerns the NHI community has identified, inventory, lifecycle management, secrets rotation, revocation, and least-privilege access, are real and necessary. Without a Warrant architecture in place, NHI governance frameworks represent the responsible interim position.

The argument is narrower and more precise than a rejection of NHI practice. It is that the credential is carrying a governance function it was never the right instrument for, and that function has a proper home: the Warrant layer, evaluated at the execution boundary, traceable to human principals, exhaustible by design.

When that layer exists, the credential returns to what it was always meant to be: an identity instrument that establishes provenance and enables attribution. Useful. Necessary. Insufficient as a governance instrument, which is precisely why it should never have been asked to serve as one.

THE GOVERNANCE ARCHITECTURE IN ONE PARAGRAPH

In a Ward-centric system, authority traces to the Ward as bearer of consequence. Where accountability is required, it traces to a named Principal as bearer of liability, but the Principal is optional. What is never optional is the Ward. The machine requires neither. It requires an identifier to anchor the evidence chain and a Warrant to anchor the governance chain, single-use, evaluated at the execution boundary, exhausted immediately upon execution. The Warden Enforcement Plane makes this a structural invariant rather than a policy aspiration. The machine is never a governance object. It is an instrument through which human-authorized actions are executed and recorded.

> **Machines don’t need identity. They need a Warrant.**