

A GATHID LABS SERIES: PART 3

Daily Trust: A Smarter Path to Identity Governance

When Light IGA Leaves You in the Dark: How to Regain Visibility Without Starting Over

Light IGA is attractive for a reason. It's built into tools you typically already own and use, such as Microsoft Entra. It doesn't require lengthy implementation cycles. It ticks the boxes on basic compliance needs, including provisioning, deprovisioning, and access reviews. And for small to mid-sized organizations with mostly cloud-native systems, it might be enough.

But for many other organizations, Light IGA falls short of what deeper identity governance requires.

For many organizations, Light IGA is a solid start, but not the finish line.

They've rolled out Entra or Okta IGA. Maybe they've built out some provisioning rules, stood up access reviews, and trained a few business owners. But now the questions get harder:

- Why does this user still have access to three disconnected systems they no longer use?
- Why can't we see who has privileged access across OT, HR and finance platforms?
- Why are our roles multiplying instead of consolidating?
- Why don't we have visibility of non-human identities like AI agents and bots?
- Or worse, why does this user still have access to this system, even though they have been terminated in the HR or contractor platform?

These are governance questions that Light IGA was never designed to answer.

From Lifecycle to Visibility

What Light IGA delivers is important: basic lifecycle management, role-based provisioning and access review campaigns. The problem is, Light IGA works on assumptions: that your roles are clean, your access policies align with actual user behavior, and that your environment doesn't include legacy applications, operational technology, or complex access hierarchies.

When those assumptions break, the entire governance model weakens.



As a result, Light IGA often falls short:

- **It doesn't detect drift**, particularly when real-world access deviates from policy
- **It doesn't handle disconnected systems**, especially those outside core directories or modern SaaS
- **It can't model toxic role combinations** or predict unintended access overlaps
- **It assumes you're managing a set of connected systems**, rather than sprawling environments with layers of identity complexity

The result is called **partial identity governance**: you may have checked the box but haven't solved the problem.

In many organizations, Light IGA delivers quick wins, and then hits a ceiling, constraining progress over time. The problem is that once you've deployed Light IGA, and it fails to deliver, you're left with two options:

1. **Rip and replace**, which is unpalatable
2. **Supplement**, which is difficult to achieve without duplicating effort and cost

This isn't a theoretical concern. We've spoken with multiple organizations who implemented Light IGA tools only to discover—months or even years later—that they had critical access gaps, stale roles, and missing coverage for AI, non-human identities and legacy or high-risk systems. In some cases, the tools were working as designed. The issue was that the design didn't reflect the complexity of the real environment.

Most organizations are hybrid, dynamic and fragmented. M&A activity, re-organizations, distributed operations, introduction of AI agents and non-human identities, and evolving business models mean the identity landscape is constantly shifting.

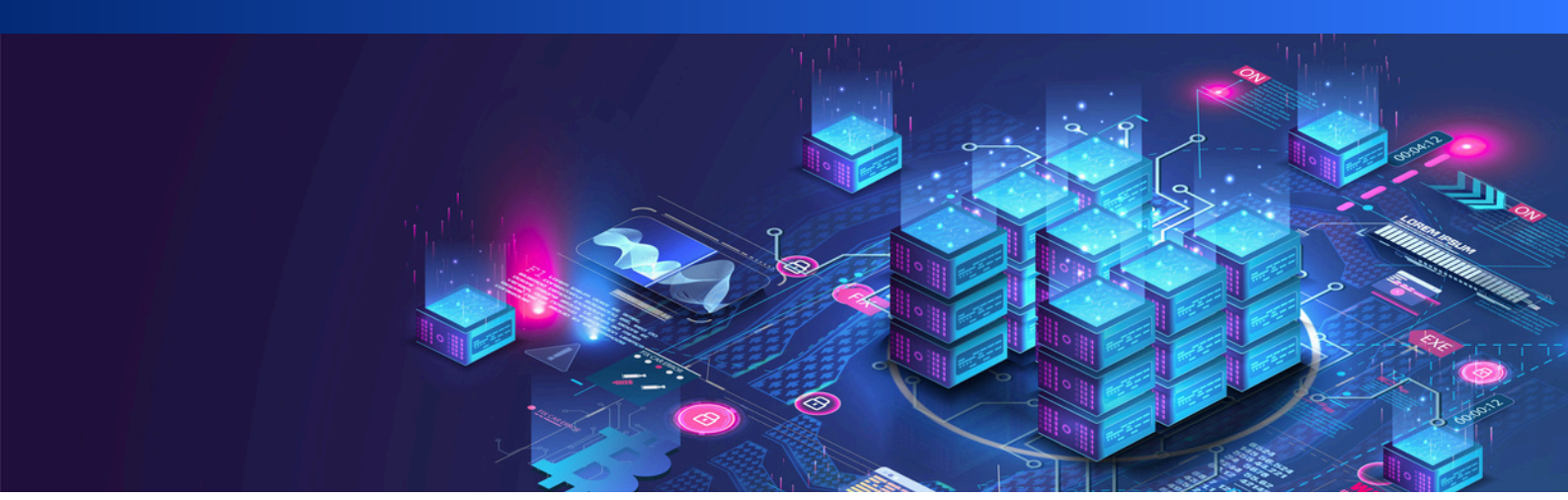
That's where Light IGA reveals its limitations. It's easy to deploy, but difficult to extend or scale. It simplifies the surface, but lacks the depth needed for true governance and visibility.

Enter Gathid: A Daily Digital Twin of Your Identity Landscape

Gathid isn't another IGA tool. It's the governance intelligence layer that Light IGA lacks. With Gathid, you don't need to abandon your Light IGA investment. Instead, we enhance it. At its core, Gathid is a daily digital twin of your identity landscape, modeled using advanced knowledge graph technology. This means Gathid doesn't just ingest data, it understands relationships, patterns, anomalies, and context across all sources of identity, including:

- Entra, Okta, and other IDaaS platforms
- HR systems and authoritative sources
- Legacy and disconnected systems
- Operational technology and physical access controls
- SaaS and on-premise business applications
- Custom built platforms

This creates a daily, relational view of your identity stack. Not only who has access to what, but why, whether it violates policy, and what would happen if it changed.



Why This Matters

Light IGA is great at issuing access. But it's not built to evaluate that access at scale, in context, or across a hybrid and federated environment.

Gathid wraps around your existing Light IGA stack to:

- Detect drift when real-world access no longer aligns with policy
- Model roles dynamically using real data, rather than theoretical constructs
- Surface toxic access combinations and visualize how they emerge
- Answer audit questions instantly across systems and user types
- Simulate access changes safely before making them

Most importantly, Gathid turns governance into a daily activity, as opposed to an annual review.

Gathid operates by building a daily, living digital twin of your identity landscape. It maps people, accounts, systems, roles, policies, resources, AI agents, non-human identities and changes using graph-based models. Gathid captures the real structure and relationships that exist across your environment. That means you can:

- See what's changed every day
- Understand who has access to what (and why)
- Reconstruct access histories for audit or incident response
- Continuously validate role models against real usage

This is identity governance that actually governs.

The Time-to-Trust Advantage

What makes Gathid different isn't just what it sees, it's how fast it works.

Typical Full IGA deployments can take 12–24 months. By contrast, Gathid can provide value in a few weeks. That means:

- Your team starts seeing identity risk immediately
- Your auditors see improvement before year-end
- Your business stakeholders get answers, not excuses

Instead of waiting two years to “finish governance,” Gathid lets you practice it continuously, starting immediately.

A Smarter Way to Augment

Organizations shouldn't be forced to choose between nothing, Light IGA, or a multi-million dollar Full IGA project.

There's a smarter, better path:

- Leverage Light IGA to do what it does best: provisioning, basic review and native integration
- Add Gathid to handle everything else, from advanced visibility and policy assurance, through to daily trust signals

Together, they form a rock-solid, scalable, modern and cost-effective governance fabric.

From Light IGA to Real Outcomes

Governance isn't about how many access requests you automate. It's about whether you can stand in front of your board, regulator or customer and say:

"We know who has access. We know why. We know we can prove it."

With Light IGA alone, that's a hard claim to make.

With Gathid, it becomes your default.

In the next post, we'll explore how organizations that have deployed Full IGA struggle with daily governance, and why Gathid remains essential before, during, and after those rollouts.

Next up: Blog 4: Full IGA Is Never Really Full IGA. You Still Need Gathid.

[Schedule a Demo](#) | [Learn More](#) | [Read Online](#)

