ClearSkye

WHITE PAPER

Identity Governance Has an Understanding Problem

How Clear View AI Reduces the Hidden Burden of Identity at Scale

Identity's Real Problem Isn't Automation

Identity governance sits at the center of modern enterprise security. Every employee, contractor, system, and application depends on access relationships that determine who can do what across the organization.

As digital environments expand, those relationships multiply rapidly—often faster than organizations can reasonably manage.

For years, the industry has approached identity governance as a control problem: enforce policies, automate provisioning, and ensure compliance. But in practice, identity teams experience something very different.

> **The challenge is not simply enforcing access.**
> **It is understanding it.**

Why does this person have access? What role or relationship created it? What changed recently?

These questions surface constantly—in audits, certifications, incident investigations, and routine operations. And they point to a deeper issue:

KEY INSIGHT

Identity governance is not just a control problem.
It is an understanding problem—and a bandwidth problem.

The Hidden Constraint: Understanding at Scale

Most organizations already have the tools they need: provisioning workflows, certification campaigns, and policy frameworks. Yet identity teams remain overwhelmed.

The reason is not execution—it is interpretation.

When access appears unusual, teams must reconstruct context across multiple dimensions: how access was granted, which roles, groups, or entitlements contributed, what approvals were involved, and what has changed over time.

This effort is rarely centralized. It requires navigating fragmented systems, tracing relationships, and piecing together decisions after the fact. As complexity grows, so does the burden.

> **IAM teams do not lack tools. They lack time to understand what those tools are doing.**

THE CORE CHALLENGE

The cost of identity governance is not in enforcement.
It is in the understanding required to make informed decisions.

Why Traditional AI Falls Short

AI is often positioned as the solution to complexity—automating decisions, predicting outcomes, and reducing manual effort. In identity governance, that model introduces risk.

Access decisions directly impact security, compliance, and operations. Organizations must be able to explain why access exists. Decisions that cannot be explained are difficult to audit—and even harder to trust.

> **The goal is not simply faster decisions. It is decisions that are transparent, traceable, and defensible.**

A Different Model: Clear View AI

A more practical approach begins with a different premise:

THE CLEAR SKYE APPROACH

Understanding must come before automation.

Clear View AI focuses on helping identity teams interpret access relationships, policies, and decisions—before attempting to act on them. It reduces the effort required to investigate identity data rather than bypassing that process.

Clear View AI in Practice

This is the model behind Clear View AI.

Instead of automating approvals or replacing human judgment, Clear View AI brings clear, read-only intelligence into the administrative experience—helping teams understand:

- Why access exists
- What relationships influenced it
- What policies applied
- What has changed over time

> **The result is not autonomous decision-making. It is faster, more confident decisions—grounded in context.**

WHERE IDENTITY WORK ACTUALLY HAPPENS

Identity governance is often framed as workflows—requests, approvals, certifications. But the real work happens in investigation: assembling evidence, tracing relationships, reconstructing context across fragmented systems. That is where identity programs slow down.

From Questions to Answers: Relationship-Aware Investigation

The daily work of identity governance is driven by questions—often urgent, often complex. When teams need answers, the effort is in assembling the evidence: Why does this access exist? How is it related to roles, groups, and entitlements? What changed—and when?

In Healthcare

- Why does a clinician have access to multiple EHR environments across facilities—and is that still appropriate?
- Which service accounts are interacting with clinical systems, and are their permissions aligned with policy?
- What changed in access for a user involved in a recent audit or compliance review?

In Higher Education

- Why does a former student employee still have access to administrative systems?
- How is access being inherited through nested groups across departments?
- Are there shared or non-human accounts with elevated permissions that no longer align to an active use case?

Clear View AI is designed to answer these questions directly. Instead of manually tracing access across systems, teams can see the full relationship model—across users, service accounts, groups, and entitlements—in a single, clear view.

> **Investigation becomes a matter of insight, not effort.**

The Role of Platform Architecture

The effectiveness of identity intelligence depends on where identity governance operates.

Traditional identity systems sit outside core enterprise workflows. Data must be synchronized, relationships reconstructed, and context inferred across systems. This fragmentation limits visibility—and constrains intelligence.

Clear Skye takes a different approach.

By operating natively within the ServiceNow platform, identity governance becomes part of the broader system of work—connected to IT service management, security operations, risk, and employee lifecycle workflows. This alignment ensures that:

- **Data is shared**
- **Context is preserved**
- **Relationships are visible**

AI can then operate within the same environment where identity decisions are made—without reconstructing context after the fact.

> **Platform-native governance means identity intelligence doesn't have to reconstruct context. It already has it.**

Expanding the Scope of Identity

Identity is no longer limited to people. It now includes service accounts, machine identities, groups, entitlements, and AI-driven processes—often representing the most complex and highest-risk access in the environment.

Clear Skye supports analysis across this full identity landscape today, enabling teams to evaluate not just who has access, but how that access is structured, inherited, and evolving. As identity expands, understanding it becomes exponentially more difficult—which makes closing the understanding gap essential.

From Control to Intelligence

Identity governance is entering a new phase.

The challenge is no longer enforcing access. It is understanding it—quickly, clearly, and at scale.

Most vendors focus on automating decisions. Clear Skye focuses on improving them—by surfacing the understanding and explanation behind them.

CLEAR VIEW AI IS DESIGNED TO BE:

- **Transparent**
- **Read-only**
- **Auditable**
- **Human-in-the-loop**

It does not replace governance. It strengthens it.

The Next Phase of Identity Governance

As identity complexity grows, organizations that rely on manual investigation will feel increasing friction.

The future will not be defined by how much is automated. It will be defined by how quickly and confidently organizations can understand access—and act on it.

Clear View AI represents that shift.

> **From control to context.**
> **From workflow to understanding.**
> **From effort to insight.**

THE CLEAR SKYE DIFFERENCE

By closing the understanding gap in identity governance, organizations can shift from reactive investigation to proactive understanding—freeing teams to focus on strategy, not search.

ClearSkye

Ready to turn the lights on?

Learn how Clear View AI can transform your identity governance program.

clearskye.com | contact@clearskye.com