A GATHID LABS SERIES: A STORY

Get AI Ready with Gathid

How Acme Inc. Mitigated Non-Compliant Access Risks to Enable AI Cross-Functionality

Acme Inc., a manufacturing powerhouse, was preparing to expand its AI capabilities across multiple business functions. From predictive maintenance on production lines to streamlining supply chain logistics, AI promised transformative improvements. But before Acme could harness AI cross-functionally, it faced a critical challenge: identifying and mitigating risks associated with non-compliant access.

With sensitive data and systems scattered across business functions (like operations, finance, marketing and engineering), ensuring that the right identities—whether human or machine—have appropriate access was paramount. Misaligned permissions posed compliance risks, operational inefficiencies, and potential security breaches. To address this quickly, Acme turned to knowledge graphs and digital twins to gain visibility and establish control before scaling its AI initiatives.

Knowledge Graphs: Illuminating Access Risks with Context

A key hurdle for Acme was a concern regarding what information was available to identities across its sprawling network of assets. Who (and what) had access to which systems? Were permissions aligned with roles? And were there dormant credentials lurking in the shadows?

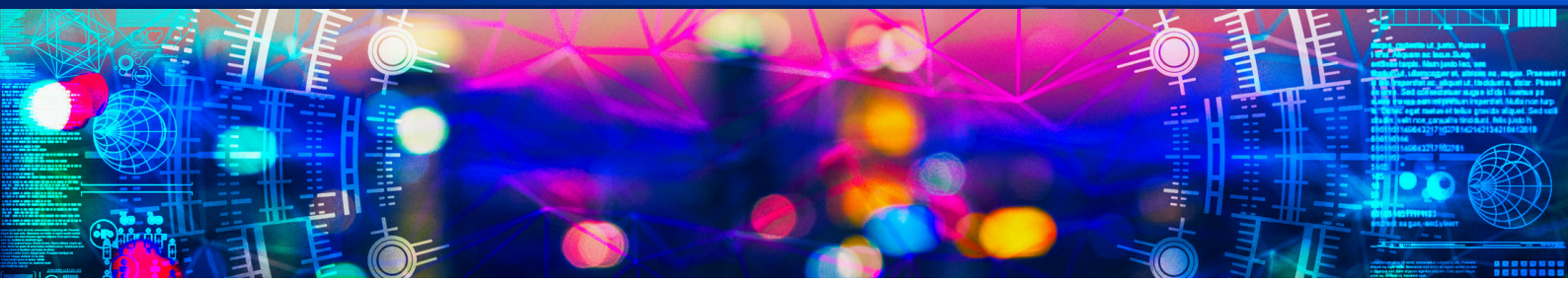
These were critical questions. Knowledge graphs provided the answers.

Acme deployed an Identity Governance application that leveraged a knowledge graph to map relationships across its identity landscape. By connecting data from HR, IT, operational technology (OT), physical access, and IoT systems, the graph created a unified view of all users—employees, contractors, machines, and AI systems—and their associated permissions.

This unified perspective uncovered access risks and areas of identity non-compliance. For instance:

- Dormant accounts for third-party external contractors who had completed projects months ago but still had access to systems and, therefore, sensitive organization data.
- Overly broad permissions for junior employees, allowing access to sensitive design schematics.
- Role combinations that allowed the same user to both create vendor accounts and approve payments to these vendors, introducing significant risks of conflicts of interest and potential for fraudulent activities.

By uncovering these issues, the knowledge graph enabled Acme to proactively identify and address potential breaches before they could be exploited unknowingly via AI and or other means.



Moreover, the graph's contextual richness allowed Acme to enforce precision in access controls. Instead of applying generic rules, Acme could tailor permissions to roles, projects, and even situational needs. For example, a maintenance robot could access production-line data but would be automatically blocked from design files or HR records.

Digital Twins: Simulating and Cleansing Access Policies

Once visibility was achieved, the next step was ensuring that new AI systems could integrate safely without exacerbating access risks. This is where digital twins became indispensable.
Policies could be run across physical and digital systems—be it a production machine, a warehouse management system, or an AI model analyzing supply chain identity and access data. Before allowing any new AI system to access operational data, Acme confirmed the levels of access for all identities were appropriate to ensure access scenarios in a safe, virtual environment.

For example, when Acme's logistics team introduced an AI system to optimize shipping routes, the digital twin modelled its users, access levels, roles, and permissions with warehouse and inventory systems. This simulation revealed that the AI's initial access included ability to read non-relevant system data, such as supplier payment records—a potential compliance risk. By adjusting permissions in the simulation and cleansing phase, Acme ensured the AI system could only access what it needed, mitigating unnecessary exposure.

Preventing Cross-Functional AI Risks

One of Acme's goals was to deploy AI solutions that could operate across business functions and applications—for instance, an AI system that analyzed both production efficiency and supply chain bottlenecks. But cross-functional AI posed unique challenges. Without clear boundaries, these systems could inadvertently bridge access between siloed data, creating compliance risks.

To prevent this, Acme integrated insights from its knowledge graph with its digital twins to simulate cross-functional AI workflows. By doing so, it uncovered potential vulnerabilities, such as:

- An AI system for inventory optimization attempting to access customer pricing data, which was irrelevant to its function.
- Overlapping permissions between marketing and production teams when the AI required shared analytics.
- An AI-driven human resources tool inadvertently accessing confidential financial performance data intended solely for executive review.

These simulations highlighted vulnerabilities and helped Acme establish dynamic boundaries for cross-functional AI. By adjusting the rules in the knowledge graph and testing them in the digital twin environment, Acme ensured that cross-functional AI systems remained compliant without sacrificing performance.

Building a Foundation for Risk-Reduced AI Enablement

Through the combined power of knowledge graphs and digital twins, Acme Inc. transformed its identity and access management strategy.

By gaining visibility into non-compliant access and mitigating risks before deploying AI cross-functionally, the company achieved several critical outcomes:

1. **Compliance Assurance**: Dormant accounts were deactivated, and overly broad permissions were reined in, reducing exposure during audits and security breaches.
2. **Precision in Access Controls**: Tailored permissions ensured every identity—human or machine—had the access it needed and nothing more.
3. **Risk-Free AI Deployment**: Simulations in the digital twin environment allowed AI systems to integrate seamlessly without introducing new vulnerabilities.

By addressing identity and access risks upfront, Acme not only safeguarded its operations but also created a scalable foundation for its AI-driven future. The company could now deploy AI across disparate systems and functions with confidence, knowing its systems were secure, compliant, and optimized for success.

For Acme Inc., the journey to AI readiness wasn't just about technology—it was about trust. Trust in the visibility, control, and precision these tools provided, ensuring that the future of AI-powered manufacturing was as secure as it was innovative.

Leverage Gathid's Specialized Identity Platform for AI-Enabled Transformation

Getting your identities and access AI-ready is not merely a technical task—it's the foundation for deploying AI responsibly and securely. The Gathid Identity Graph empowers organizations to leverage AI without compromising security, compliance, or efficiency. Our advanced knowledge graph and digital twin technology provides deep visibility and control over your identity landscape, allowing for precise management of user permissions and access.

This proactive approach ensures that AI applications do not inadvertently expose sensitive data or violate regulatory standards. By partnering with Gathid, you benefit from customized Identity Governance strategies and a dynamic, sandbox environment to test AI integration policies, ensuring they accounts and levels of access are secure before going live. Embark on your AI journey with confidence—Gathid is here to ensure your AI advancements are innovative, compliant, and secure.

Schedule a Demo | Learn More | Read Online