

Know every identity your financial customers will ask about



Linx is the AI-native identity security platform that teams in financial software trust to see, govern, and fix identity risks across human, non-human, and agentic identities.

Every new service account and AI agent is another identity your customers expect you to govern, and another line item in your next SOC 2, ISO, or PCI review. Most financial software companies can't say how many they have, let alone who owns them. All too often, access reviews run in spreadsheets and orphaned accounts go unnoticed. Linx is one unified platform for audit-ready visibility and governance across every human, non-human, and AI agent identity, in weeks rather than the years legacy IGA takes.

Ensure the right identities have the right access, to the right resources, at the right time.



Unified identity visibility & intelligence

See every human, non-human, and AI agent identity on one graph, correlating HR, IdP, cloud, and app sources to give you a source of truth for how many identities you have, who they belong to, and what they can do.



Automated access reviews with real results

Use Linx to supercharge your access reviews, with streamlined campaign creation and deep and context-driven analysis, then take action in-platform and with audit-ready evidence.



Say goodbye to standing access

Then say hello to context-aware, AI-assisted JIT access request policies that allow your organization to move quickly, but also without temporary needs leading to permanent identity risks.

Why busy teams choose Linx



Power Tool for Busy Users

Built so that security users of all kinds, not just dedicated IAM professionals, can take control of their organization's identity security.



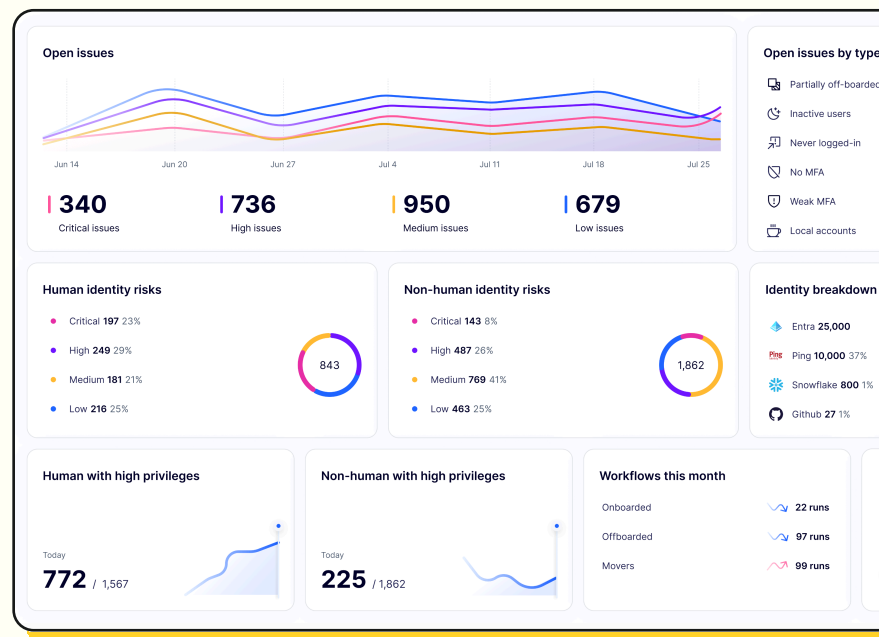
Unified Security & Governance

Replace old solutions – whether legacy IGA or scripts & spreadsheets, with a unified, future-ready platform that sees and governs all of your identities together.



Day One Value

Get audit-ready visibility and remediation in weeks, not months– or years–long timelines that leave you with more work and no operational relief.



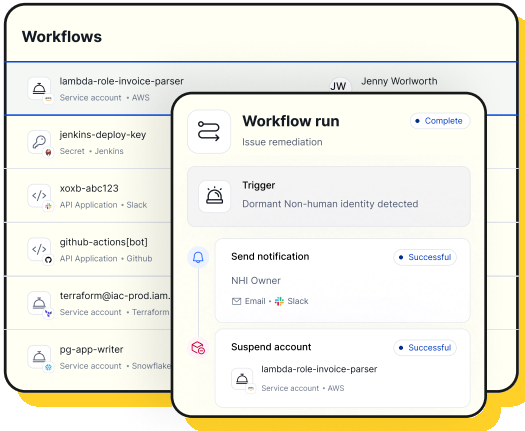
"With Linx, I can make much smarter decisions and understand exactly what I want to do before I do it. [We have created] much more autonomous, automatic processes."



Lior Zagury
Sr. Director of Global IT,
monday.com

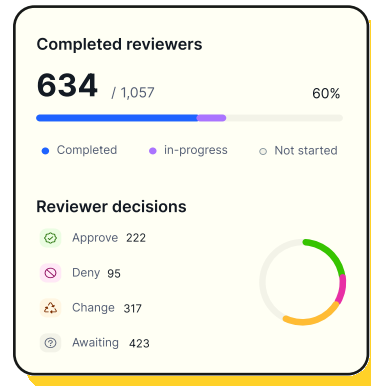
Non-human and AI-agent identity governance

The Linx platform brings non-human and AI agent identities into the same security and governance framework as every other identity in your business. With Linx, your team can automatically discover AI agents across your environment, govern them, and use the MCP Gateway for granular visibility and real-time enforcement.



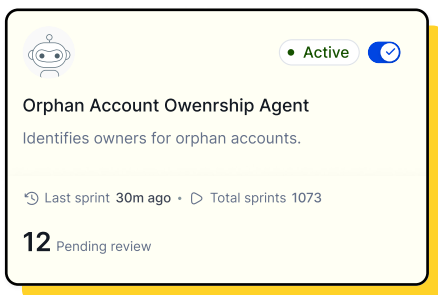
UARs built for your identity estate

Instead of assembling reviews by hand and doing tedious spreadsheet work, you can make UARs a breeze with automatic access review campaigns. Find and fix vulnerable identities directly within the platform, put an end to rubber stamping, and run your first access review in a fraction of the time other solutions require.



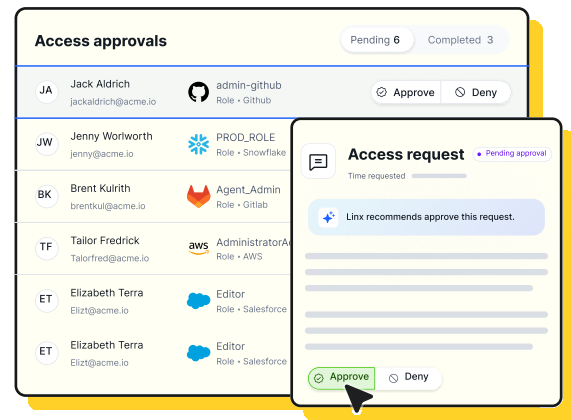
Clean up orphaned and dormant accounts

Instead of relying on incidental findings to identify dormant or orphaned accounts, Linx surfaces these risky accounts automatically. Out-of-the-box, find dormant, orphaned, unused, and partially off-boarded accounts, then actually fix them from directly within the platform.



Just-In-Time access that moves at the pace you do

For fast moving teams, a temporary need for elevated access can lead to permanent risk without the right governance tools. Security teams turn to Linx so they can replace standing privileges with time-bound, right-sized access so elevation doesn't mean permanent group membership and permanent risk.



*"My main use case for **Linx Security** is defining our identities, human, and agents. When people join the company, we manage joiners, movers, and leavers. We get full visibility of every employee and where they have access. Not only that, we can see all the agents that are in use and what access they have to what application and data source. It is a full security and governance platform."*



Product Manager

at a 1,000–5000 Employee Tech Vendor