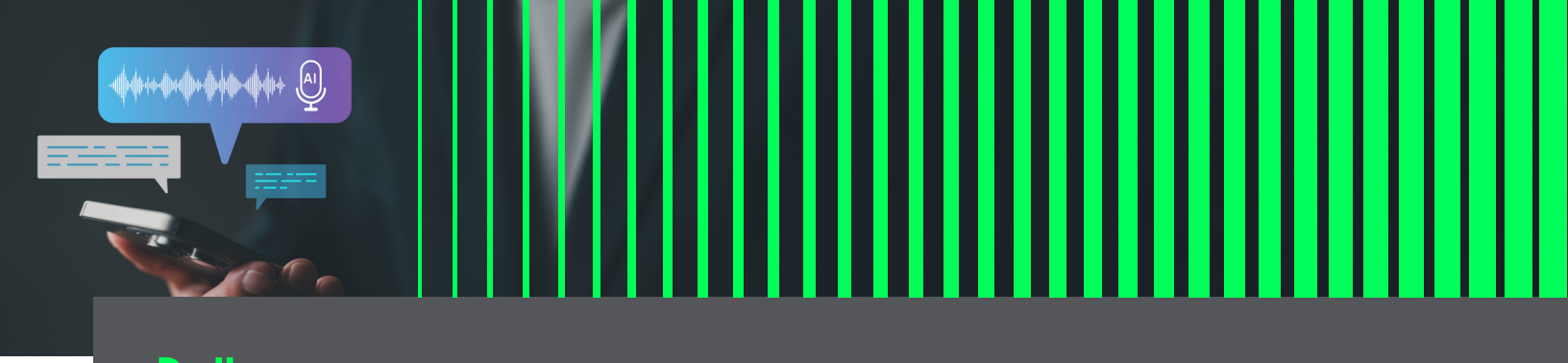

Delinea

TELNYX CASE STUDY

Telnyx secures agentic AI access with Delinea

Challenges

Telnyx first deployed StrongDM, now part of Delinea, to control and record which employees could reach the databases, Kubernetes clusters, and virtual machines that run the business. That deployment worked. Every human identity had defined access, and every session left a record.

Employees soon began building personal AI agents. Teams stood up shared, specialized agents to manage infrastructure without a person present. Within months, every employee had at least one agent, and many had several. The access model built for one human, one identity, could no longer answer a basic question: Was a person or an agent responsible for a given action?

During internal testing, one overprivileged agent deleted a Postgres database. The incident occurred in a development environment and never reached production, but it exposed a core problem: Without a distinct identity per agent, there was no way to know whether a person or an agent had taken the action, and no way to limit what it could reach in the first place.

Solution

Realizing the agent access challenge is the same as the human access challenge, Telnyx extended the existing Delinea deployment to cover agent identities the same way it already covered human ones. Every identity, whether human or agent, now runs through the same control plane. That control plane enforces runtime authorization, verifying every identity at the moment it requests access rather than granting standing permissions in advance. It delivers the following outcomes:

Telnyx by the numbers

- **140+ AI agents** in active use across the organization
- **500 human and agent identities** managed through one control plane
- **Seconds to trace** any infrastructure action back to the responsible service account and identity type, human or agent

Telnyx builds and sells voice AI agent infrastructure to other businesses. Speech recognition, language model inference, and text-to-speech run on GPU compute co-located with the telephony network, so AI agents respond to callers in real time. Underneath that infrastructure sits a global carrier network carrying voice, messaging, and SIP trunking across more than 100 countries.

A company that sells AI agent infrastructure to other businesses had to solve, internally, the same identity and access problem many of those businesses now face. How does an organization secure access when the identity requesting it might be a person, or might be an autonomous agent acting on behalf of that person?

telnyx

- **Scoped access:** Agents run under team-level service accounts with limited access, separate from the humans who built them. Per-agent identity, a more granular model, is the direction Telnyx is building toward next.
- **Accountability:** Every session leaves a record for the databases, Kubernetes clusters, and VMs StrongDM brokers, including when an agent acts on its own while its owner is away from the keyboard.

The result is a single access model: defined access, recorded sessions, and a clear answer to whether a person or an agent was responsible for a given action on Telnyx infrastructure.

> The biggest thing that Delinea is doing is giving us auditability and insight into what our agents are doing when we are away from our keyboards
>
> → Dhruv Kumar, Technical Product Manager, Telnyx

Result

Telnyx now manages every identity, human or agent, through one control plane. The audit trail identifies whether a person or an agent was responsible for a given action, rather than folding both into a single shared identity.

That capability showed up in practice when an alert fired and an agent accessed the environment to deploy a fix on its own. The agent's access was authorized at that moment, not provisioned in advance. Afterward, the team reviewed exactly what the agent had done in the StrongDM session logs, the kind of review that was not possible before every identity ran through the same control plane.

Telnyx applied the same discipline to agent access that it already applied to human access, while many organizations are still deciding how to handle agent identity.

Looking ahead

The shift from one identity per human to one human orchestrating several agents is not unique to Telnyx. It is a change that most organizations putting AI agents to work inside their infrastructure will face.

The Postgres incident made that clear: The question was not whether agent identities needed their own access controls, but whether the team would wait for a production failure or move first. For most organizations, that shift means moving from standing access to runtime authorization: checking each identity the moment it acts, not before.

Telnyx acted early, rather than waiting for a larger incident to force the decision. That experience offers a preview of the identity and access questions every one of those organizations will eventually have to answer.

Delinea

Delinea is the identity security platform that governs what humans, machines, and AI agents do once they have access. It enforces just-in-time authorization at the moment of action, not just when access is first granted, reducing reliance on standing privilege across on-premises, multi-cloud, and ephemeral infrastructure. Built on deep privileged access management expertise, the Delinea Platform continuously discovers identities, analyzes risk, and enforces least privilege, so every access decision is defensible. This gives organizations the visibility and control to adopt AI with confidence. Learn more at **delinea.com**.

