

Benevity strengthens data privacy control while accelerating DevOps workflows

How Benevity's site reliability engineering team scaled infrastructure access during its move to AWS

✔ Challenges

The company's technology stack includes Microsoft SQL Server and EC2 in AWS. Before deploying Delinea runtime authorization, a custom Ansible script provisioned access approval requests for individual user server accounts. This would've been manageable with one or two users, but the processes did not scale with the business. Shell access to EC2 also required SSH keys, so they needed a way to drop key management altogether. The AWS migration was the moment for Benevity to adopt a more scalable approach to managing infrastructure access. The site reliability engineering (SRE) team had three requirements that any solution must meet:

- Faster access for users
- No manual steps in the access approval process
- Compliance with recognized security standards

✔ Solution

For secure database access for developers, Benevity's SRE team uses Delinea runtime authorization for role-based permissions and audit logs on backend systems, giving the company and its clients real visibility into who touched what data, and when.

Delinea runtime authorization met Benevity's needs for simplicity and security, and changed how it granted access to users. Database access became Delinea runtime authorization's most heavily used feature almost immediately.

Benevity brought in a few developers to test the platform, and it was a positive experience for them. The company's VP was a strong advocate and was sold the first time he saw it. The security team valued the auditable access to databases, and Benevity could retire previous ways of access, like shared SSH keys.

Background

Benevity provides corporations with a way to cultivate a culture of purpose, meaning and impact through software that connects their people with the causes they care about, whether that is donating their time, their money or a simple act of kindness. To date, Benevity has processed nearly \$8B in donations and 43 million hours of volunteering time to support 326,000 nonprofits worldwide. The company's solutions also drove 530,000 positive actions and awarded 1.2 million grants worth \$12B. Benevity takes security and compliance seriously to assure its clients, many of which have large, sophisticated privacy and security protocols of their own, that data is protected.





[Delinea runtime authorization] StrongDM is just easy to use. We were able to get it set up and connected without having to ask for help. And now we can do things like retire SSH key sharing, easily provision access to databases, and provide our security team with auditable access to every single DB query.”

→ Nina d'Abadie, Director of DevOps, Benevity

✓ Results

With Delinea runtime authorization, Benevity automates the internal approval process for provisioning database access and standardizes permission levels across teams of developers with role-based access. The security team leans heavily on Delinea runtime authorization audit logs.

Now, developers can spin up an on-demand database with scrubbed data, but with a production schema. They have an on-demand, generic dataset that is fully representative of production, a huge improvement, since dev environments rarely match production. They can test complex scenarios and run performance tests. They spin it up on demand and have the access they need automatically provisioned without going through additional teams. It is completely self-service.

Benevity has auditable access to databases and shell access, and was able to retire previous ways of accessing systems such as shared SSH keys. The security team can see the audit logs of every query, and who ran it, which is what compliance reviews ask for.

“We have a really neat use case for [Delinea runtime authorization]: Getting developers access to the databases, but in particular, access to scrubbed datasets. We had a team collaboration where they built some cool scrubbing scripts via Lambda that would do a database pullback and scrub it, and this was all tied into [Delinea runtime authorization] via Terraform. That meant all of these new databases would be registered into [Delinea runtime authorization] StrongDM as they're pulled back. Now we could easily provide access when spinning up ephemeral databases,” said Nina d'Abadie, Director of DevOps at Benevity.

Delinea is an identity security platform governing what AI agents, humans and machines can do, and for how long. Just-in-time authorization extends privileged access management from access to action, cutting standing privilege across on-premise, multi-cloud and ephemeral infrastructure. Its platform scores identity risk and keeps access decisions auditable. Over 9,000 organizations, including two-thirds of the Fortune 100, rely on Delinea. Learn more at delinea.com.