

Bullhorn Moves Closer to Zero Trust with Delinea Runtime Authorization

How Bullhorn automated access based on roles, let engineers keep their preferred database clients and simplified audit processes

✓ Challenges

Before implementing Delinea runtime authorization, Bullhorn used a different access management solution to control access to MS SQL databases. As Bullhorn's product offerings expanded, so did its infrastructure complexity, with new database types such as MySQL, Postgres and Oracle.

Over time, the team ran into latency, frequent disconnections, weekend outages and unmanageable access workflows. For a small team on an on-call rotation, the outages were especially frustrating.

William Vu, Infrastructure Network Security Manager, says one of the most common triggers for a weekend escalation was the previous provider going down. Reliability was always something to keep an eye on.

End users complained of a sluggish experience, especially when accessing remote databases via appliances, which were often hosted separately from the resources they were meant to secure. The previous solution's complexity made it increasingly difficult for the DevOps and security teams to manage.

Vu says the previous solution worked well enough when Bullhorn was smaller, but as the number of cross-functional users grew, it became a headache. The team was constantly juggling licenses, and the user experience did not meet expectations.

✓ Solution

When Bullhorn decided it was time to scale up, it evaluated multiple platforms. Delinea runtime authorization stood out for its simplicity, and the team liked that it let them keep their own clients without sacrificing auditability.

Background

Bullhorn provides recruitment software solutions. As its internal infrastructure expanded, the company needed to manage access without compromising security or operational efficiency.

The company employs more than 1,400 people. Its technical environment is complex, with 16 product offerings and a footprint spanning multiple public clouds, including AWS, GCP and Azure. It operates under the SOC 2 and ISO 27001 compliance frameworks.





With [Delinea runtime authorization] StrongDM, our users can now leverage any SQL client they prefer, whether it's MS SQL, MySQL Workbench, or others. That kind of flexibility made a huge difference for us."

→ William Vu, Infrastructure Network Security Manager, Bullhorn

Its lightweight, agentless architecture was easy to deploy and maintain while still offering strong audit capabilities. Engineers could use their preferred database clients, a significant improvement over the previous provider's restrictive Remote Desktop Protocol (RDP) sessions.

Delinea runtime authorization let Bullhorn automate and centralize access management across its entire infrastructure. Under the previous setup, constant license juggling meant engineers frequently lost access when sessions timed out. Role-based access control (RBAC) and automated access workflows eliminated the problem.

That automation reinforced the principle of least privilege (PoLP) across Bullhorn's environment and helped the company move closer to its zero trust security goals.

The switch to Delinea runtime authorization was smooth. The proof of concept (POC) was so straightforward that Bullhorn moved the POC environment directly into production with minimal effort. Vu says the Delinea support team was always available and most of the legwork was done before the purchase. Onboarding was so easy that Bullhorn did not need its professional service hours.

✓ Results

With Delinea runtime authorization, Vu says weekend reliability is no longer something Bullhorn has to worry about.

Bullhorn can now automate access based on roles, and offboarding is as simple as removing a user from the single sign-on (SSO) provider.

Bullhorn also needed a solution that could simplify SOC 2 and ISO 27001 audits and provide detailed session logs. Delinea runtime authorization's audit capabilities, including query logging, exceeded expectations.

Vu says the previous solution produced session recordings that were of limited use. Nobody was going to sit through hours of footage to work out what code someone typed, or most likely pasted, into the query field. With Delinea runtime authorization, he says, the team knows exactly what is being done on the databases. It captures every query and keystroke, which he calls "huge" from a compliance perspective.

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.