strongdm

State of Enterprise Database Access

2023 REPORT

More Databases, More Problems

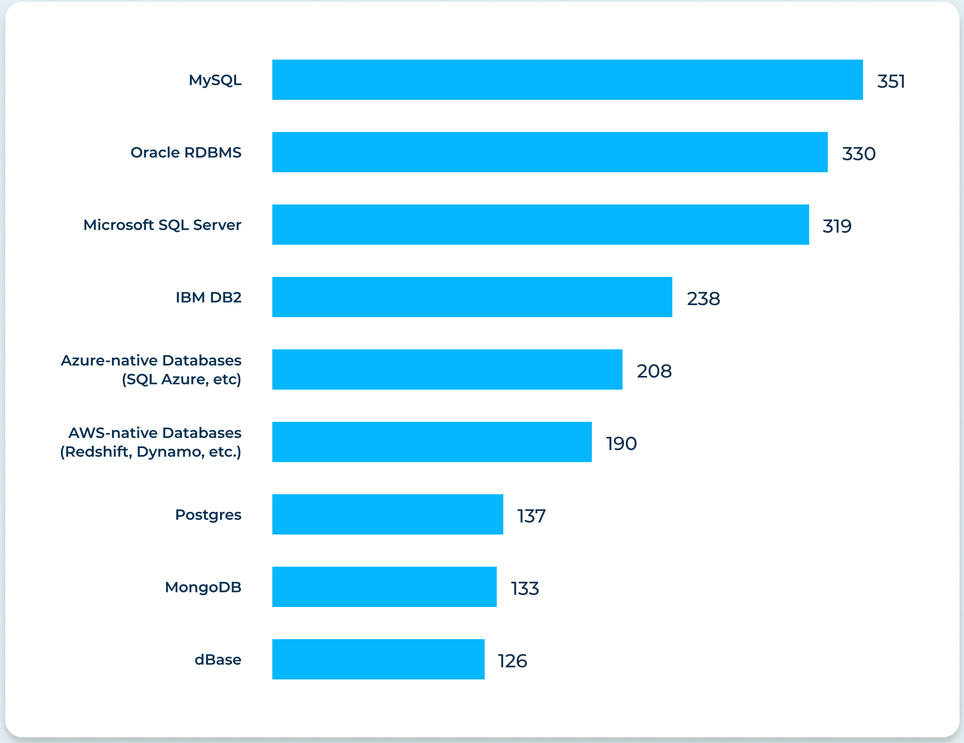
Databases are a permanent fixture of every organization's tech stack. Whether they're relational, NoSQL, columnar, vector, graph...the list goes on, they're foundational to your ability to build and develop applications and products.

In fact, the latest count shows that there are **400 different databases** between relational and NoSQL alone. One problem has only gotten worse as databases and their supporting teams have grown over time: Access.

While databases are great at what they do–managing data–ease of use with regards to access has always been an afterthought. For example, if you're technical enough to use a database, then using a python script or CLI to login shouldn't be a problem.

The result? DBAs and other users can face substantial barriers and lost productivity as they go about their job. This is true even across the most popular databases in use today.

Most Used Databases in the Enterprise

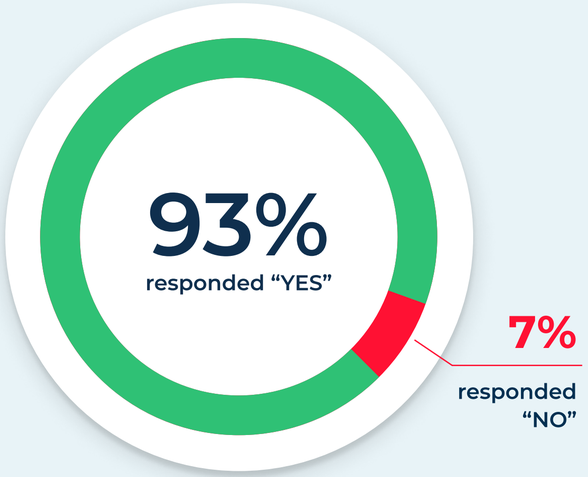


Pain in the Access: Database Access

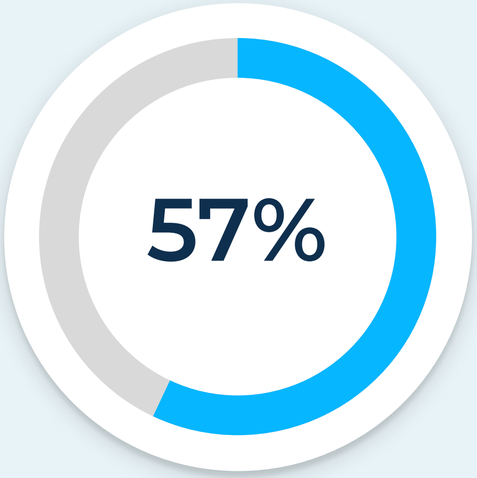
Managing access to databases is a recognized issue. In fact, in a recent survey, 57% of respondents listed databases as one of the most difficult technologies for managing access. Furthermore, over-provisioning is a real challenge for organizations trying to move quickly and enable teams to do their jobs. 93% of organizations state that technical staff has access to sensitive infrastructure, including databases.

Following the Great Resignation, ensuring that access has been revoked from former employees, that zombie credentials do not exist, and that new and existing employees have “right size access” has never been more important to preventing breaches. This is especially true for databases and any organizations that are beholden to GDPR or CCPA.

Do you have technical staff that has access to sensitive infrastructure (servers, clusters, databases. cloud APIs, etc.)?



Number of organizations that name **databases** one of the most difficult technologies to manage access to.



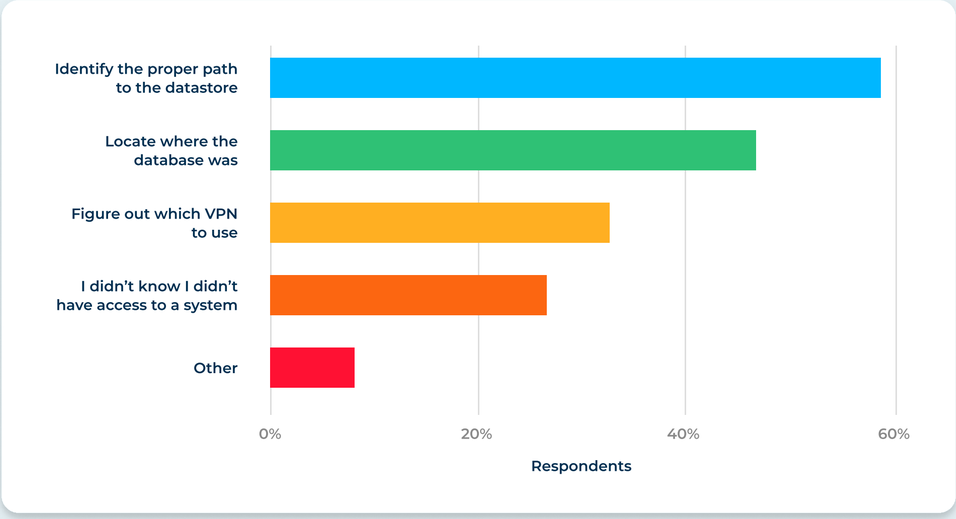
Difficult Data Access, Difficult Job

Challenges facing database access are not limited to granting or revoking access. According to the **2022: Year of Access Survey**, 59% of organizations name identifying the proper path to a datastore as a main reason they're blocked from accessing infrastructure. An additional 47% name simply locating a specific database as a challenge. What's worse—53% of teams claim having been held accountable to missed deadlines for projects, regardless of if they had the access they needed or not.

This indicates that not having a comprehensive view of all available datastores, and then being able to quickly and easily provide access to each one, can have a detrimental impact on projects, as well as on a DBA's or engineer's career.

> "It doesn't matter that you didn't have the right access—the deadline was still missed."

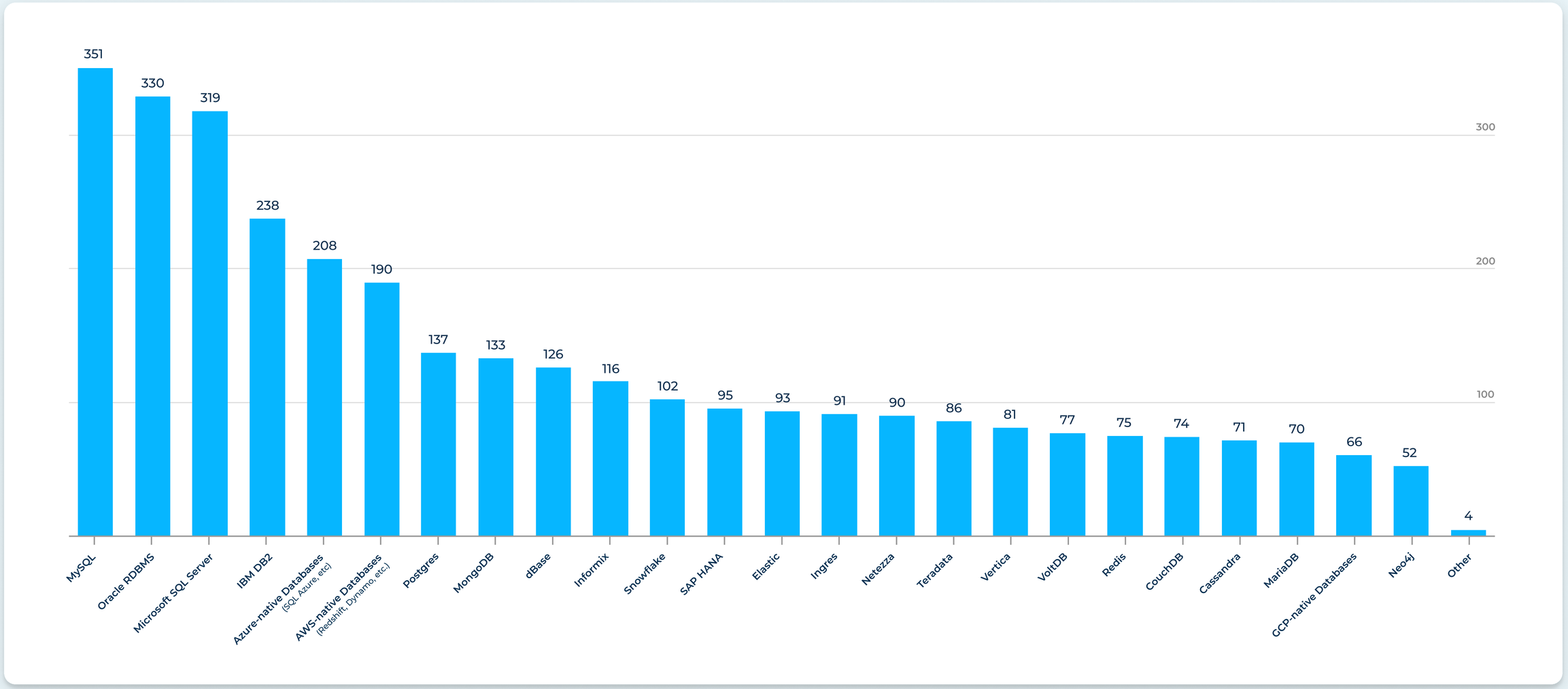
When you're blocked from accessing infrastructure, it's usually because you couldn't...



53%

of teams report being held accountable to missed deadlines, even if caused by the inability to get access to the required infrastructure.

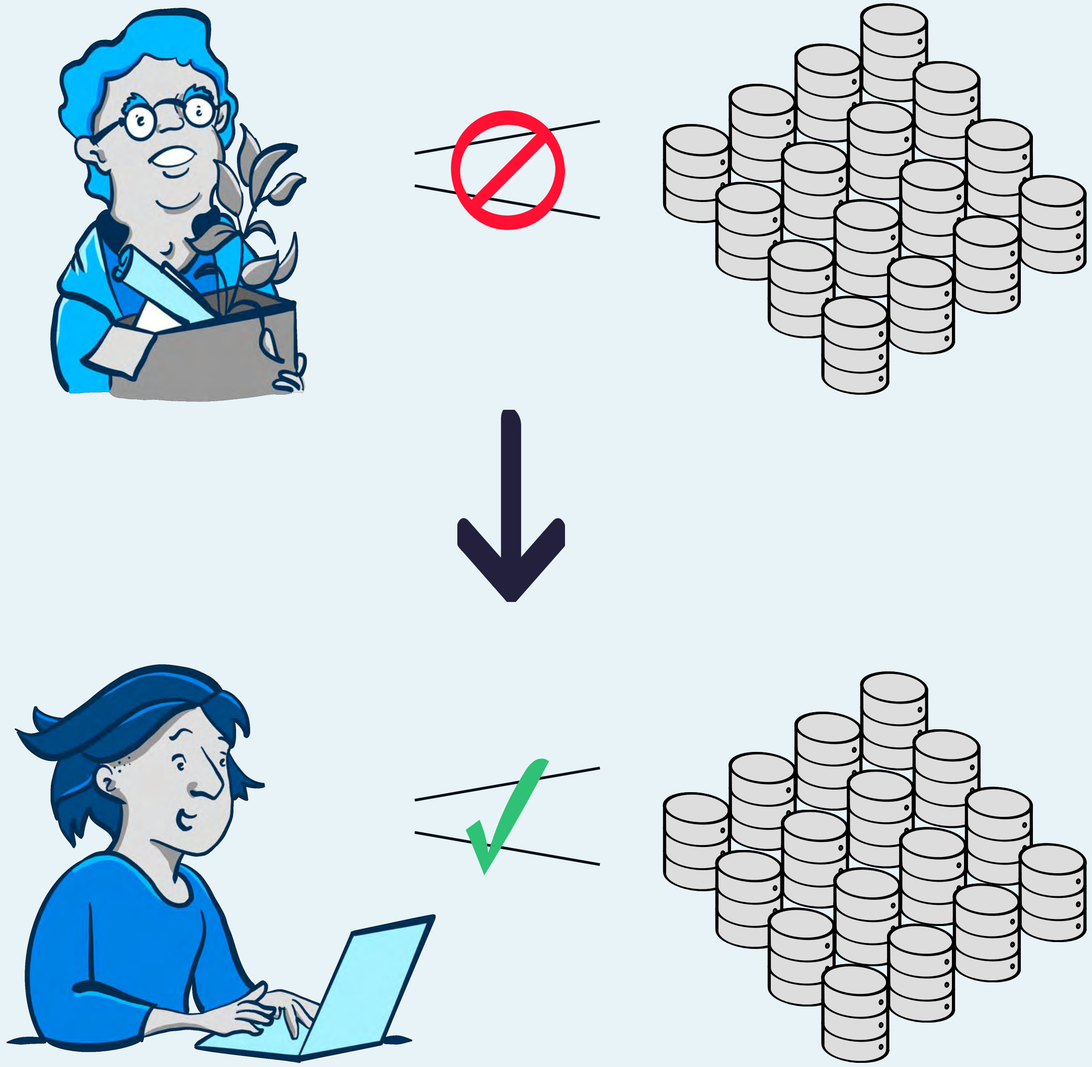
Most Used Databases in the Enterprise



Database Access at Scale is Untenable

According to **Forrester**, an enterprise DBA can support as few as 8 and as many as 275 databases, averaging at about 40. But what happens when that DBA leaves? Taking the average, that's 40 databases that need to have access revoked. And when a new DBA is hired? Now 40 databases need to be provisioned.

This approach is not scalable, especially as new databases continue to be adopted into the enterprise. Every new database, every new DBA, and even new projects have overhead associated with provisioning and managing each database.



Getting to Simple and Secure Database Access

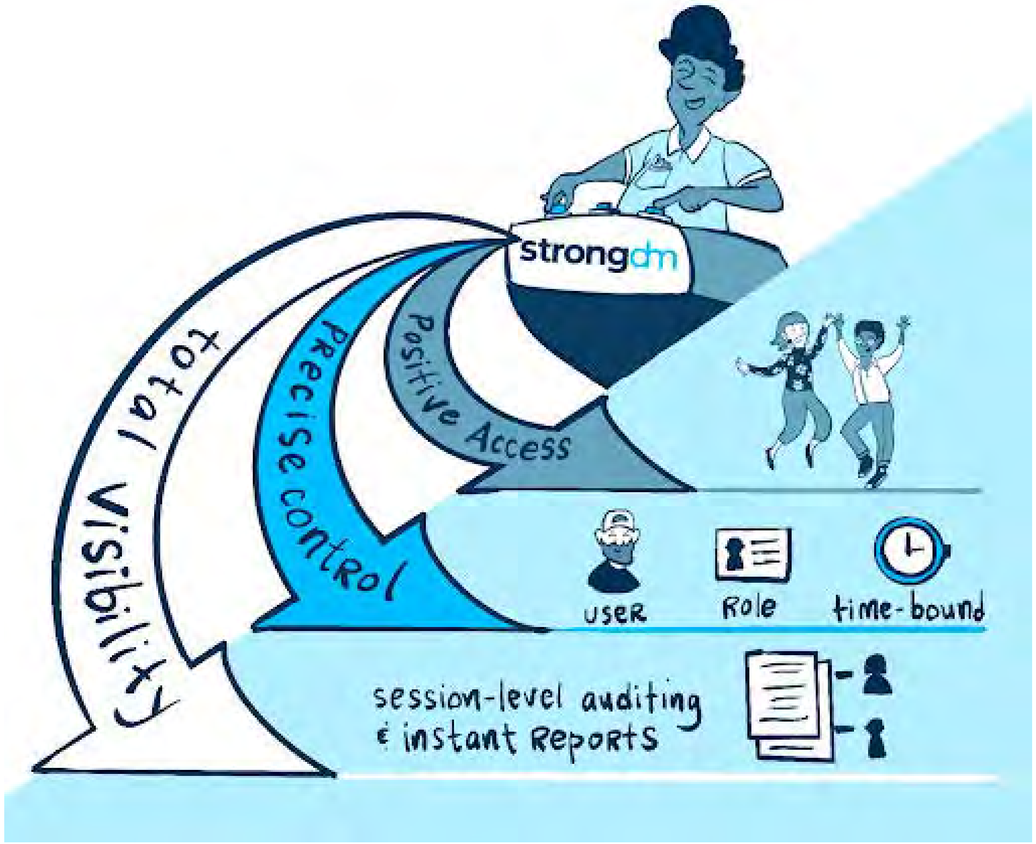
Improving database access has a few key requirements. You must have total visibility, precise control, and embrace idea of confident access—employees can and should have access to the tools they need to do their jobs. And this must be done across all databases and database types in your environment.

Total Visibility provides organizations with the ability to see who has access to each database, as well as track what queries were run, when each happened, and what data was accessed by each employee.

Precise Control delivers granular controls over who has access, when that individual has access, and the ability to shut off access to all systems immediately is critical to ensuring that data is protected.

Both of these come together to deliver **Confident Access**, which provides:

- Just-in-Time access to every database
- Visibility into all queries and who had access when for audits
- Immediate revoking of access as needed



How Consolidating Access Improves Data Management

Olive AI: Improving Database Access (and Security) with StrongDM

Olive

About Olive AI

Olive provides an AI and process automation solution designed specifically for the healthcare industry.

> **From a compliance point of view, I have no users in my data layer. And from a security point of view, having the ability to have line-by-line, high-fidelity audit trail of all access to core databases, saved in an immutable infrastructure is a security and compliance person's Holy Grail, and we got that with StrongDM.”**

Vivek Desai
SVP of Engineering, Olive AI

Challenges

- As the company grew, its processes for granting, managing, and auditing database access became cumbersome and unsustainable
- With up to 300 users in the database layer at any given time, making it difficult to manage employee database access
- VPN provisioning was required for snowflake or one-off database access requests

Results with StrongDM

- Olive standardized and simplified access to their databases, wrestling in improved security
- End users and developers are on-boarded on day 1, and it’s no possible to provide read-only access to certain databases
- The organization went from up to 300 users in the database layers to zero users in the database layer
- Olive now has a high-fidelity, line-by-line audit trail of all access to core databases
- Olive was able to retire it’s VPN and rely on StrongDM to manage all database provisioning and access management

About StrongDM

StrongDM's People-First Access platform provides technical staff with direct access to the critical infrastructure they need to be productive. The company was founded on the principle that databases and data access must be secure, while also easy to access, and has since expanded to cover critical infrastructure. StrongDM customers enjoy easy and secure infrastructure access regardless of tech stack or environment. Trusted by the Fortune 500 to fast-growing businesses like Peloton, SoFi, Chime, Yext, and Betterment, StrongDM delivers the fast, intuitive, and auditable access required for DevOps and modern security and compliance. Connect with us on **LinkedIn**, **Twitter**, **Facebook**, and **YouTube** or head to **www.strongdm.com** to learn more.

Ready to address infrastructure access? Sign up for a free, no-BS demo today.

Sign up today

strongdm