How Regulated Organizations Secure Infrastructure Access

How financial and data-driven organizations secure sensitive infrastructure access with StrongDM.

strongdm
Now part of Delinea

Table of Contents

Infrastructure Access in Regulated Environments

Organizations operating in regulated industries must balance strong security controls with the need to support productive engineering and infrastructure teams. Managing access to infrastructure while maintaining auditability and compliance becomes increasingly complex as environments scale.

The organizations in this guide demonstrate how teams modernized infrastructure access while maintaining strong security oversight and compliance readiness.

Axos Financial Secures and Streamlines Database Access with StrongDM

Axos Financial, the holding company for Axos Bank, Axos Clearing, and Axos Invest, faced significant challenges in managing database access and streamlining hundreds of thousands of access requests.

The Problem

Axos Financial struggled to manage database access efficiently amidst rapid growth. They faced the daunting task of annually reviewing over 200,000 database permissions, creating a significant operational burden for their managers.

The Solution Before StrongDM

Initially, Axos relied on individual access requests, resulting in a cumbersome process where users filed multiple tickets for database access. They implemented a Role-Based Access Control (RBAC) approach to streamline this process, but further improvements were needed.

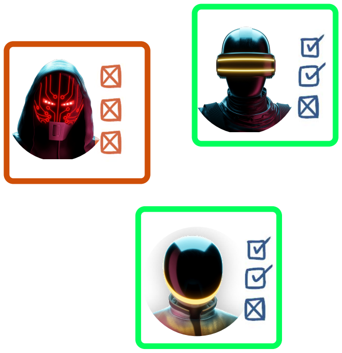
> "
>
> If someone is looking for a quick approach to secure how access is being provisioned and they want to make that maturity improvement very quickly, I would tell them to look at StrongDM because of how easy it is to use and how easy it is to deploy and roll out. It will help them leapfrog the access improvements they need or want to make in their programs."
>
> Raghu Valipireddy
> *SVP*

The StrongDM Difference

Axos turned to StrongDM to manage database access securely and efficiently. With StrongDM, they consolidated multiple access requests into a single, role-based request, eliminating direct database access. StrongDM provided an additional security layer and comprehensive audit logs, significantly enhancing their operational and security posture. The user-friendly platform also ensured high adoption rates among employees, facilitating a smooth deployment and effective access management.

Database Access Overload: Managing Access at Scale

Amid rapid growth, the prospect of reviewing and attesting 200,000+ database permissions on an annual basis by 200 managers posed an overwhelming challenge for Axos Financial. They needed to redesign the database access management model to keep pace with company growth, and creating a system of efficient access processes without compromising data security was critical for SVP Raghu Valipireddy. "Our intention was to figure out how to manage the risk from an operational and security standpoint—that's what drove us to StrongDM." - Raghu Valipireddy, SVP, Axos Financial



Organized Onboarding: From 50 Access Requests to 1

Over half of Axos Financial employees are considered technical users. With a highly technical user base, provisioning database access to them during onboarding was particularly cumbersome. It wasn't uncommon for some to require access to as many as 50 databases. In the past, users had to individually file 50 separate database access tickets because there was no construct of role.

Axos implemented a **Role-Based Access (RBAC)** approach to streamline the provisioning process and reduce the number of access requests per database. Users now make a single request in the StrongDM platform and receive all the appropriate access for their roles. Raghu Valipireddy said, "[New users] don't even need to enter a password because it is AD authenticated. So, once they log into the computer, they can interact with databases."

Bolstering Security by Eliminating Direct Database Access

From a security standpoint, Axos was able to eliminate direct database access. Users now must go through StrongDM, which serves as an additional security layer between users and databases, removing direct database access and providing visibility into access patterns.

Because StrongDM captures audit logs at the gateway level outside the database, Axos has an audit trail detailing who accessed which database and what they queried without impacting the performance of the database. "If we need to investigate a security incident, these audit logs are extremely useful to gain visibility."

StrongDM: Easy to Use, Easy to Deploy, Easy to Roll Out

While researching database access management options, the Axos team met with multiple solution providers, but the user-friendliness of the StrongDM platform stole the spotlight. According to Raghu Valipireddy, "At the end of the day, if it doesn't get adopted and if it doesn't get used by our employees, we're not even making the slightest progress from a security standpoint… StrongDM is the most customer-friendly of all the solutions, and it's easier to use than anything else we have seen. We've seen Teleport and many other database security products in the market right now…" Raghu added, "You guys listened to what we really needed and helped us break it down into small pieces, and you brought in a lot of the folks internally… You took those notes and went back and fought for us from an engineering standpoint. And you helped those features get prioritized internally."

Deploying Scalable Database Access

Strategic partnership was a key theme throughout the deployment. Axos collaborated closely with their StrongDM Customer Success Manager, who listened to the specific challenges and acted as the voice of the customer to the StrongDM engineering and product teams.

Together, steps were taken to make feature enhancements and address specific needs proactively. When asked about the customer support and onboarding process.

Ready to write your own StrongDM success story? **Book a demo**.

> "
>
> **Throughout my career within the access space, I've bought a number of tools, and I would honestly say the experience I had from the onboarding perspective at StrongDM is the most impressive I've seen compared to any other company. I've worked with all of those big vendors from an onboarding standpoint, but nobody has done such an impeccable job of assisting with onboarding compared to StrongDM.**
>
> axos FINANCIAL | **Raghu Valipireddy**
> *SVP*

Cherre Adopts Zero Standing Privilege with Confident Access Controls

Cherre is the leader in real estate data and insight. The company connects decision-makers to accurate property and market information and helps them make faster, smarter decisions. Cherre's mission is to connect all real estate data and make it accessible for better investment, management and underwriting decisions. Some of the largest investors, asset managers, banks, and insurance companies in the world use Cherre to power their data and insights.

> "
>
> Because we use StrongDM for multiple services, it creates consistency in how we manage the access. Whenever someone asks, 'How do I get access to such and such?' The answer is always StrongDM, so people know what to expect."
>
> **Ben Lipton**
> *Senior DevOps Engineer*

Hypergrowth Prompts Immediate Need for Centralized Access Platform

Cherre experienced a massive surge in revenue and sophistication during a hypergrowth stage. It needed an auditable access platform to organize access requests for managers, eliminate over-privileged accounts, and simplify compliance processes with advanced logging protocols. The company also wanted a single solution that could manage access across all of its modern infrastructure, including Kubernetes clusters and databases.

Efficient Access Controls Boost Productivity

Ad hoc access requests were bogging down engineering managers with a constant stream of requests to databases and Kubernetes clusters, so Cherre enlisted StrongDM to turn chaos into order.

StrongDM automates the responses to each request based on a set of rules determined by the admin. Whether it's granting access immediately, limiting the duration of the access with temporary access, or reaching out to a manager for approval; the admin sets the policy and StrongDM provides the access. This new system enabled team leaders to focus on more pressing tasks and increased productivity across the board. Engineers received just the right access exactly when they needed it. Director of Engineering, Mike Gruen, noted, "[StrongDM] makes it easier for people like me, who are on the management side, to go in and quickly approve temporary access requests. We've been able to increase who can approve privilege escalations."

Improving the Mean Time to Investigate (MTTI) was also a priority for Cherre. At the time, investigations were manual and time-consuming without a tool that clearly showed which engineers had access to production clusters. Now it's easy to see who has access to specific clusters, play a session recording, and even remove access with StrongDM.

Making Compliance Scalable

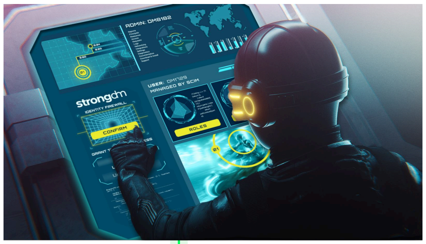
As Cherre's customer roster grew to include larger and more data-heavy customers, so did the frequency of audit requests. With StrongDM, Cherre is now able to track evidence collection, log every query to simplify SOC 2, complete annual audit frameworks, and meet monthly customer auditing requirements. "The audit logs are an important part of our compliance story. We have manual procedures that need to be performed on our database, but the fact that those procedures are logged makes us feel a lot more comfortable about that access," said Ben Lipton, Senior DevOps Engineer, Cherre.

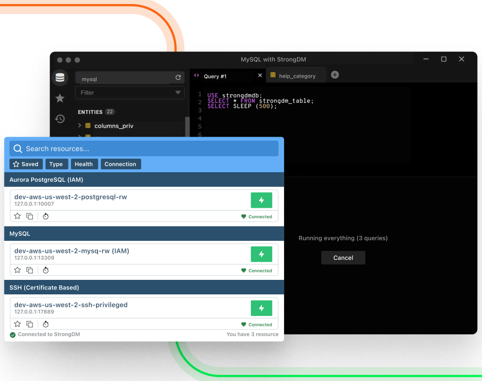
Confident Access Helps Reach Zero Standing Privilege

After implementing StrongDM, every role follows uniform access rules within the easy-to-use console. For read-only items, Cherre now has a role to standardize persistent access across its engineering team. For right-sized access, it even has the ability to apply temporary access grants when and where they're needed.

The deployment and adoption of StrongDM was a smooth and painless process. According to Ben, StrongDM helped the engineering and security teams at Cherre find the simplest way to "say yes to access" which means happier, more productive teams. And because StrongDM never shares credentials with end users, they are more secure too. "...StrongDM does a lot to keep things simple that could be complex. For example, if you just give StrongDM access to all of the networks where you will need to access resources by deploying gateways, it handles the networking for users to reach out to your resources. StrongDM just does what you think it's going to do," Lipton concluded.

> "
>
> **It would be almost impossible to track what people were doing on the database and within the Kubernetes clusters without a tool like StrongDM.**
>
> cherre | **Ben Lipton**
> *Senior DevOps Engineer*





```
USE strongdmdb;
SELECT * FROM strongdm_table;
SELECT SLEEP (500);
```

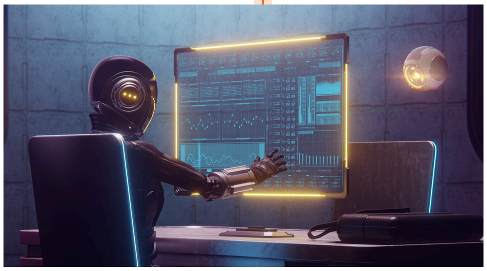
Aurora PostgreSQL (IAM)
dev-aws-us-west-2-postgresql-rw
127.0.0.1:10007
Connected

MySQL
dev-aws-us-west-2-mysq-rw (IAM)
127.0.0.1:13309
Connected

SSH (Certificate Based)
dev-aws-us-west-2-ssh-privileged
127.0.0.1:17889
Connected

Connected to StrongDM
You have 3 resource

Running everything (3 queries)



Better.com Adopts Zero Trust Access Policies

better.com

41	5	2,000
Databases	Different DBMS	Employees

Better uses StrongDM to conveniently enforce access controls for SOC 2 & ISO27001 compliance.

> "
>
> For Zero Trust, StrongDM is an amazing tool. BYOD, within the company, outside, wherever you need to go, you can access data in a secure way.
>
> better.com | Ali Khan
> *CISO*

StrongDM Provides Secure Access for a Distributed Workforce

Prior to StrongDM, Better didn't really have a strong management system for database access. Everything was very manual. With StrongDM, it's much easier to grant access and audit access control.

Better was able to implement it within a day. Within a week they saw more and more users requesting access to it once they saw how easy it was to access databases.

"Before StrongDM, it would take up to a week to get someone provisioned. With StrongDM, we can now do that in minutes."
- Ali Khan, CISO

Better Shifts to Proactive Data Loss Prevention

StrongDM helped Better shift from reactive to proactive approach to data loss prevention. By detecting suspicious behavior in real time (ex: query after hours, or double expected query volume) they are able to suspend users before potential damage is done.

Audit Functionality Accelerates Incident Response

StrongDM's audit functionality provides peace of mind that every permission change and employee query is automatically logged and instantly accessible.

If an incident ever occurred or an auditor asked, Better would have all the evidence necessary to begin an investigation without delay.

Security And Compliance Outcomes

Across these organizations, several common outcomes emerged:

- Improved visibility into infrastructure access activity

- Simplified audit preparation and compliance reporting

- Reduced reliance on shared credentials

- Better control over access to sensitive infrastructure resources

Modernizing Infrastructure Access

These organizations demonstrate how modern SaaS companies can simplify infrastructure access while improving security, visibility, and operational efficiency. StrongDM helps engineering and security teams manage infrastructure access across databases, servers, Kubernetes clusters, and cloud platforms.

strongdm

Now part of Delinea