We Solved the Infrastructure Access Problem

These 10 companies solved the infrastructure problem. You can too. These are their stories.

strongdm

Table of Contents

In this ebook, you'll learn how several organizations, from growing startups to established enterprises, solved the access problem using StrongDM. These stories offer an insider's view of the unique challenges each organization faced, digging into details with the software engineers, DevOps directors, and InfoSec leaders who found the solutions. Read on to discover the tricks and tools they used to improve productivity, streamline compliance, simplify onboarding, and so much more. The answers may surprise you.

Coveo Unites Infrastructure Access and Auditing with One Platform to Rule Them All

COMPANY 01

Coveo is a market-leading AI-powered relevance platform that aims to enable customers like Adobe, Humana, Workday, and Salesforce to offer relevant experiences. Its SaaS-native, multi-tenant platform injects search, recommendations, and personalization solutions into every digital experience. The R&D team needed a way to manage access to over 100 multi-regional databases that didn't involve managing 100 usernames and passwords per technical employee.

With StrongDM, Coveo's administrators and developers get just-in-time, least-privilege access to every database they need, regardless of protocol or location, from a single control plane and a single credential. Coveo's technical staff were able to save time on manual workflows, and eliminate any associated security risks. This enables them to spend more time on more important projects—such as hardening AWS resources, and intrusion and anomaly detection. Plus, the Coveo team now has complete visibility across their entire stack with centralized and granular audit logs and simplified compliance audits.

> "StrongDM is the one solution to rule them all. You simply integrate all your datasources into StrongDM; you integrate all your servers into StrongDM; you integrate all your Kubernetes clusters into StrongDM. You give your developers one simple tool they need to connect using SSO, and they have access to what they own."
>
> **Jean-Philippe Lachance**
> *Team Lead - R&D Security Defence*

The Limitless Stack Creates Untenable Access Workflows

Coveo Relevance Cloud(™) is a search platform that creates a unified index of content from tools like Google Drive and Gmail, and then integrates with various application platforms like Salesforce, SAP, Adobe Experience Manager, and Zendesk. This allows disparate types of content to be available and ranked by relevance through one simple search bar. The Coveo Relevance platform provides solutions for ecommerce, service, website, and workplace applications and provides tangible value to customers by helping them drive revenue growth, reduce customer support costs, increase customer satisfaction and website engagement, and improve employee proficiency and satisfaction.

Coveo was founded in 2005 as an on-premises solution. By 2012 it was offering a multi-tenant service, with separate accounts for development, production, and HIPAA. Coveo maintains SOC 2 and HIPAA compliance and is working to implement the ISO 27001 standard.

Coveo expanded from one database and one region to over 20 databases per environment, per region—including Amazon RDS, Aurora, mySQL and PostgreSQL, based on DevOps team preferences. Managing access rights for that many databases wasn't easy. And as Coveo grew to become a multi-regional company with a data residency offering, the number of databases expanded exponentially. One highly privileged employee might have 100 unique usernames and passwords for the 100 databases they needed to access, all stored in a password management tool. It was challenging to keep up with password changes and software updates—and it was clear that Coveo needed a better access and security solution.

Coveo Gains the Ability to Audit Everything

The Coveo team initially built an in-house solution. After a few years, the team decided to have a look at Teleport and HashiCorp Boundary, but found that each tool only had part of the solution, not the complete package. For example, having an audit trail was critical for security.

"What I really needed was the audit trail," says Jean-Philippe Lachance, Team Lead–R&D Security Defense at Coveo. "For us, it was the most important thing to have. For security analysis, for SOC 2, and for HIPAA compliance, we need to be aware of all the operations that happen inside an environment. We need the ability to audit everything. We need the ability to go back and see what happened on a specific instance, the ability to go back and see the queries on a given day. The audit trail using StrongDM's gateway is way more efficient than having to go configure each data source one by one."

Teams Save Time Without Sacrificing Security

Coveo began using StrongDM in 2021, to centralize the employee login process and allow each employee to access every tool they needed from the central StrongDM console. Now, the onboarding process for new hires is simple. Instead of provisioning credentials to each of the hundred databases, employees get one credential to access everything they need.

Implementing StrongDM has also reduced the amount of administrative work for DevOps teams. Whenever new infrastructure is provisioned, all permissions are automatically assigned through StrongDM using Terraform and the StrongDM API. By unifying all infrastructure access in their SSO, Coveo eliminates the administrative work of fielding lost-password requests. Instead, the team can focus on top-priority initiatives and projects.

"I need to work on intrusion detection, anomaly detection, AWS account management, hardening those databases, and hardening our AWS resources," says Jean-Philippe "Even if we had more developers, if we did not have StrongDM, we would need to just say no to new projects. That would greatly impact our ability to grow."

Olive Elevates Data-Layer Security Above Compliance Standards

COMPANY 02

Olive provides an artificial intelligence and process automation solution designed specifically for the healthcare industry. As the company grew, its processes for granting, managing, and auditing database access became cumbersome and unsustainable. As a cloud-first and HIPAA-compliant organization, Olive required robust auditability and controls across their entire stack. Additionally, Olive's flexible workforce model, The Grid, gives employees the ultimate flexibility to work from anywhere, but also means the company needs stringent security and access controls to protect sensitive data. The Olive team knew they needed a modern and scalable approach for infrastructure access.

Since adopting StrongDM, Olive has been able to accelerate on-boarding for technical new hires, deployed fast and auditable least-privileged access across their remote workforce, and achieved the "holy grail" of security postures—high-fidelity, query-by-query visibility into actions in databases and critical systems.

> "From a compliance point of view, I have no users in my data layer. It's a phenomenal security posture. I can go with my head high to any healthcare organization in the world and tell them the data layer security is on par with and above most stringent regulatory requirements.
>
> Olive | Vivek Desai, *SVP Engineering*

Before StrongDM

Custom workflows and insufficient controls create bottlenecks and compliance gaps

Olive, an artificial intelligence and process automation solution designed specifically for healthcare, serves over 40 healthcare organizations that encompass more than 600 hospitals in 41 states across the U.S.—including a growing number of health systems with AlphaSites (onsite centers for AI workforce operations). Olive helps healthcare systems like Tufts Medical Center automate patient pre-registration for COVID-19 tests, decreasing patient wait times and increasing testing capacity.

When Olive was launched, the company primarily managed database access with Ansible. The team constructed and maintained YAML files with lists of database users and their required access for databases, individual tables, entire clusters, and more. Then, they executed the appropriate Ansible playbooks to apply the changes to the clusters. Access to customer systems (RDP into Windows server) required connecting to Olive's corporate VPN and then RDPing into a server via business-to-business (B2B) VPN tunnel. The team audited data access via custom scripts, usually written in Bash or Python.

"Granting, managing, and auditing bespoke database access was becoming very difficult," says Infrastructure Engineer, Kellen Anker. "Data access requests were usually snowflakes or one-offs."

Olive's existing standards and policies governing data and customer-system access needed to be updated to keep pace with the company's hyper-growth. Accessing Olive's private databases required connecting to the corporate VPN and authenticating with individual user credentials. "User credentials were stored as encrypted Ansible variables," says Anker.

"It was difficult to keep track of who was already in our Ansible automations, and who was not, without decrypting and inspecting each of these config files. Managing usernames and passwords for Olive's engineers quickly became unruly." Furthermore, Olive's corporate VPN had become a bottleneck for network performance for nearly every employee.

Accessing Olive's customer systems required per-customer networking settings, in the form of AWS route tables and NACLs. This quickly led to a bloated cloud environment, and added unnecessary complexity to a system already plagued with scalability concerns. The Olive team also recognized an opportunity to improve auditability and controls around customer system access, which would come as a significant compliance win.

Olive's CloudOps, Infrastructure, and DataOps teams faced challenges managing employee data access. The Security team didn't have a complete understanding of the scope of employees' access to data. IT had the headache of provisioning VPN accounts for one-off database access requests.

StrongDM Natively Supports Olives Entire Stack

When Olive Senior Infrastructure Engineer Michael Plemmons suggested StrongDM as a potential solution, the team carefully evaluated StrongDM and another potential vendor. One reason the team chose StrongDM was because it supported Olive's entire stack, including RDS, Redshift, DynamoDB, Athena, and RDP access to customer systems.

Olive's Cloud Infrastructure team found that the benefits of StrongDM include standardized, simplified access to databases, higher security, and uniquely responsive customer support.

"StrongDM saved my team time by not having to create one-off users for each database and has allowed us to standardize our access control patterns," says Anker. "It has also been time-saving for ramping up new engineers who need to access all our data sources. With one command, they can start contributing."

End Users Experience Seamless Access

"StrongDM's vastly superior UX was a major factor in the decision," says Anker, who successfully pitched the solution to Olive's leadership with Senior Vice President of Engineering, Vivek Desai. "End users no longer need to worry about authentication to individual data sources, and requests for new data access are easier to fulfill. The UX for our customer support engineers—those who RDP into customer-hosted systems—has simplified tremendously for similar reasons. Managing up to dozens of login credentials for every server was unruly and error-prone; StrongDM has eliminated the need to manage these entirely."

StrongDM has made it possible to get developers on-boarded and working on day-one, as they no longer have to wait for corporate VPN access and have a single, standard login with access to everything they need. It's also possible to give developers read-only access to certain databases, which Desai says can help them become better engineers, by simply seeing how other teams and individuals organize their database schemas.

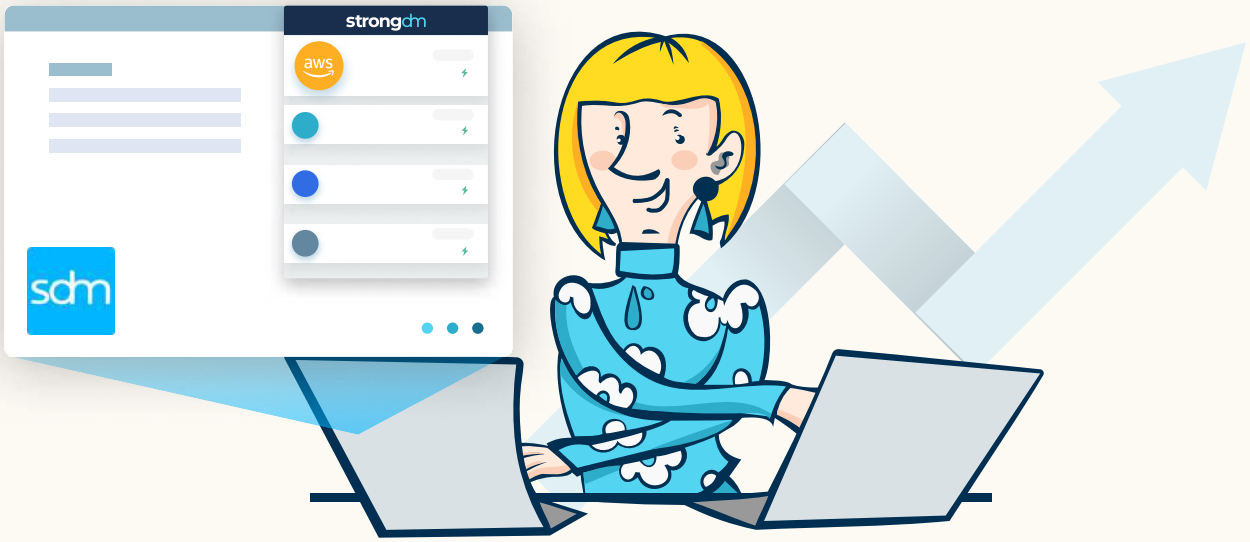
"StrongDM is an end-user-centric way of looking at accessing sensitive systems," says Desai. "It puts the end user first and it also adds modern methodologies and deployment patterns into the mix."

High-Fidelity Auditing Simplifies Compliance

“From a compliance point of view, I have no users in my data layer,” says Desai. It’s a phenomenal security posture. I can go in with my head held high to any healthcare organization in the world and tell them the data layer security is on par with, and above, most regulatory requirements.

Previously, there would be up to 300 users in the database layer at any given time, but now everything is managed through StrongDM.

“And from a security point of view, having the ability to have line-by-line, high-fidelity audit trails 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. On top of that, very critical systems are recorded in full fidelity. Having that streamlined into an easy-to-use, deployable product is awesome.”



Ironclad Shrinks Attack Surface and Onboarding Time using Google Groups Integration

Ironclad

COMPANY 03

Ironclad is leading the charge to free up legal professionals from administrative work. It focuses on turning contracts into business assets, allowing teams to extract valuable information to drive business decisions. By choosing StrongDM, Ironclad freed up its own professionals to focus on improving its product, rather than manually managing infrastructure and user access.

> "The access control has helped us out the most. And with audit logging, it's very easy for the auditors to see what queries are being run by a particular person at a particular time. That granular level auditing–I can't stress enough how big of a win it is.
>
> Ironclad | Nate Schlitt, *software engineer*

Unified Access Reduces Costs and Improves Compliance

Ironclad struggled with two main issues: managing endpoint access and auditing activity. VPNs were expensive from both a budget and maintenance perspective. They required significant effort to maintain, but didn't provide the evidence auditors required to fulfill SOC 2 compliance requirements. Specifically, VPNs were not sufficient to prove that Ironclad prevented unauthorized access to its databases. As Ironclad evaluated options, they needed a solution that could fulfill SOC 2 requirements and support its entire backend stack, including the DBMS from a recent acquisition.

Granular Auditing Improves Visibility

A few employees at Ironclad used StrongDM at previous companies. They recommended it because it was easy to set up–particularly on the Kubernetes side. Ironclad did its due diligence, and their decision-making team of five made a unanimous choice. They chose StrongDM for its ability to conduct granular auditing and grant temporary access to resources. And they liked that StrongDM integrates with G Suite and allows the team to forward logs to Datadog and set up Slack alerts.

Query logging and SSH replay sessions are some of the most useful features, according to Nate Schlitt, Software Engineer. The team can see what the user typed and the commands executed.

"Just being able to see everybody's queries against the database–that granular level auditing, I can't stress enough how big of a win that was," Schlitt said. "Being able to see every user's query, connection access, and network access is fantastic."

Automated Access Speeds Up Onboarding

The most significant benefit for Ironclad has been the time saved **onboarding new users**. Ironclad uses Google Groups, and when a user is added to the Google Group, they also get automatic access to resources via StrongDM. The team can drag and drop a new user into a role that matches the Google Group, automatically assigning access. This ensures least privilege permissions are assigned by default for all new hires. Before StrongDM, any new accounts and local provisioning had to be manually configured.

With StrongDM, Ironclad reduced the **attack surface** in two ways. First, the company no longer distributes database credentials to staff. Instead, staff authenticate using Google. As a result, the underlying credentials can't be compromised because they are never stored locally on staff workstations. Ironclad also restricts access to isolated subnets by leveraging StrongDM's egress-only proxy that ensures traffic only communicates with the proxy. This protects the back end systems from unauthorized access.

Best of all, by reducing its administrative overhead with StrongDM, Ironclad now has more time and energy to help legal professionals streamline their own work.

Benevity Elevates Data Privacy Control and Accelerates DevOps Workflows

COMPANY 04

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 it's to donate their time, their money, or just do a simple act of goodness or kindness. To date, Benevity has processed nearly $8 billion in donations and 43 million hours of volunteering time to support 326,000 nonprofits worldwide. The company's solutions also facilitated 530,000 positive actions and awarded 1.2 million grants worth $12 billion. As such, Benevity takes security and compliance seriously to assure its clients'—many of which have large, sophisticated privacy and security protocols of their own—data is safeguarded.

For secure database access for developers, Benevity's site reliability engineering (SRE) team uses StrongDM for enhanced role-based permissions and audit logs on backend systems, providing visibility and due diligence that brings the company and its clients peace of mind.

> "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 DBs query.
>
> Nina d'Abadie
> *Director of DevOps*

StrongDM Provides Scalable Role-based Access

The company's technology stack includes Microsoft SQL Server and EC2 in Amazon Web Services (AWS). Before deploying StrongDM, access approval requests for individual user server accounts were provisioned through a custom Ansible script. This would have been fine for just one or two users, but as the company scaled its business they needed to scale their ability to maintain secure workflows and processes at the same time. Additionally, shell access to EC2 required SSH keys, so they needed a solution that would also help streamline and create efficiency in this area.

During the process of migrating to AWS, Benevity wanted to figure out a more scalable approach to managing infrastructure access. The SRE team had three core requirements that any solution must meet:

1. Users must gain faster access
2. Access must be automated and not include a manual access management process
3. The system must uphold industry-leading security standards

"We had some really great demos with StrongDM," says Nina d'Abadie, Director of DevOps at Benevity. "We brought in a few developers to test it out, and it was a really positive experience for them. Our VP was a strong advocate for it and was sold the first time he saw it. Security was appreciative of the auditable access to databases, and we could retire previous ways of access like shared SSH keys."

StrongDM was able to meet Benevity's needs for simplicity and security, and helped streamline how it granted access to users. Furthermore, once Benevity began using StrongDM, the biggest use case quickly became database access.

Devs Gain Self-service Access to Scrubbed, Production-like Data

"We have a really neat use case for StrongDM: 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 StrongDM via Terraform," d'Abadie says. "That meant all of these new databases would be registered into StrongDM as they're pulled back. Now we could easily provide access when spinning up ephemeral databases."

Now, developers can spin up an on-demand database with scrubbed data, but with a production schema. "Developers now have an on-demand, generic dataset that is fully representative of prod—a huge improvement, given that dev environments aren't always representative of production. So now they can do different use cases, test complex scenarios and datasets, and also do performance testing. They spin it up on-demand and have the access they need automatically provisioned without going through additional teams. It's completely self-service," d'Abadie adds.

Benevity Saves Time While Boosting Security

With StrongDM, Benevity now automates the internal approval process required to provision database access. It also allows Benevity to leverage role-based access in order to standardize permission levels across teams of developers. StrongDM's audit logs have also proven to be extremely useful to the security team.

"By using StrongDM, not only do we have auditable access to DBs and shell access, but we could retire some of our previous ways of accessing, like shared SSH Keys," says d'Abadie. "For the security team, the compliance aspect and being able to see the audit logs of every single query that was run and everyone that accessed it—that's incredibly valuable," added d'Abadie.

MakeSpace Streamlines Onboarding & Offboarding

COMPANY 05

Faster Onboarding Supports Rapid Growth

MakeSpace has experienced the sort of hyper-growth that every startup dreams of. After growing revenue by 150% in the past year, MakeSpace raised $30M in new funding. To support that growth, the engineering and analytics teams doubled in size.

The engineering team grew frustrated by how much effort it took to onboard new hires and manage ad hoc requests for infrastructure access from on-call support. Instead of maintaining a dozen one-off scripts, they wanted a solution that offered the convenience of an SSO.

> "The team at StrongDM has been exceptional. We haven't had many support requests at all because the product just works the way that it's supposed to.
>
> MakeSpace | Ted Conbeer, *SVP of Strategy*

Convenient Controls Enforce PoLP

StrongDM made it possible to enforce the principle of least privilege (PoLP) without bogging down Makespace's engineering team with administrative work.

StrongDM replaced a dozen scripts with a single command to onboard new engineers. Offboarding is equally painless.

> "The challenge of managing database permissions only gets exponentially worse as the team scales. As we've scaled, we get more and more value out of StrongDM because it doesn't get more complicated.
>
> MakeSpace | Ted Conbeer, *SVP of Strategy*

Auditing Supports Total Transparency

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, Makespace would have all the evidence necessary to begin an investigation without delay.

Troops Manages Just-in-time Access Without Sacrificing System Uptime

COMPANY 06

Devs Need Access to Terabytes of Customer Data

The world's largest sales teams rely on Troops for real-time insights into the status of their deals. To generate those insights, Troops ingests terabytes of customer data. Being proactive about data security was incredibly important from day one.

Troops needed to tightly manage and monitor access to customer data without decreasing developer productivity.

> "Huge fan of this product. It really eliminates the traditional headaches with giving teams database access with the right level of granularity and auditing. StrongDM is a staple tool for any dev team.
>
> TROOPS | Greg Ratner, *Co-Founder and CTO*

Troops Pursues SOC 2 Ahead of Schedule

As Troops began to work with more of the Fortune 1000, customers asked them to complete more rigorous security RFIs and SOC 2 compliance. To demonstrate their commitment to security, Troops decided to pursue SOC 2 compliance earlier than expected. But the process can be pretty painful and require over a year to complete. As a fast-growing startup, Troops needed to complete SOC 2 under a tighter timeline without distracting the team.

> "We were able to roll [StrongDM] out to the entire company literally within an hour.
>
> TROOPS | Greg Ratner, *Co-Founder and CTO*

StrongDM Streamlines Compliance

Troops turned to StrongDM to speed up the process. StrongDM made it easy to enforce SOC 2 policies and gather evidence proving those policies are in place. For example, all users must authenticate using MFA and reauthenticate after a defined idle time.

Because StrongDM automatically logs every user creation/deletion, permission change and query, Troops saved significant time and effort gathering evidence to answer auditors' questions.

Braze Enforces SOC 2 Policies with StrongDM

COMPANY 07

Braze Commits to Multiple Compliance Regimes

Braze powers personalization for the world's most recognizable brands. Since Braze sends over 10 billion custom messages to consumers every month, data security is a top priority. A key component of Braze's security strategy is a commitment to multiple compliance regimes, including SOC 2, ISO27001, and GDPR.

StrongDM Simplifies Access Controls

Fulfilling these compliance requirements is an enormous undertaking for Braze's engineering team. The team turned to StrongDM to simplify the process.

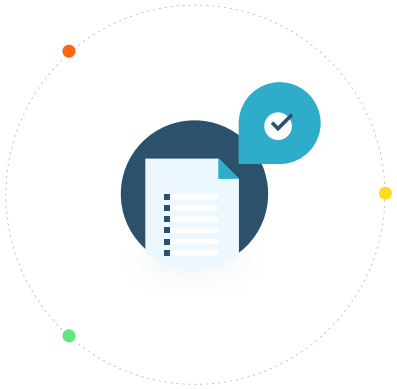
StrongDM reduced the logistics to manage permissions to a single command. No need to manage multiple scripts anymore.

> "We deployed StrongDM, and within the first 3 days we actually had more than 160 databases that we had already added to the StrongDM console. It really simplified our workflow."
>
> Jonathan Hyman
> *Co-Founder and CTO*

> "We used StrongDM to instantly deliver results to our auditors, which really simplified the SOC 2 process."
>
> Jonathan Hyman
> *Co-Founder and CTO*

Teams Instantly Answer Auditors' Questions

StrongDM also reduced the effort to gather evidence to prove access controls are enforced. By automatically logging every user creation/deletion, permission change, and query, Braze can now instantly answer auditors' questions.



Better.com Adopts Zero Trust Access Policies

COMPANY 08

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

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.

> "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*

> "Before StrongDM it would take up to a week to get someone provisioned. With StrongDM we can now do that in minutes.
>
> better.com — 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.

Yext Goes Public After Achieving SOC 2 Compliance

COMPANY 09

StrongDM filled that pivotal role of being able to provision the access, keep track of what's going on and give us that central pane of control.

StrongDM Provides Secure Access for a Distributed Workforce

Prior to StrongDM, Better didn't 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.

> "The effort to achieve SOC 2 compliance without StrongDM would have been a monumental effort, not only in terms of resources, but in terms of cost.
>
> Michael DaSilva
> *Manager, Information Security*

Central Control Plane Improves Visibility

Yext powers location data for some of the most recognizable brands. After a dozen years of hard work, the company went public in 2017 with revenue of over one hundred and twenty million dollars.

Achieving SOC 2 compliance represented a key step in the IPO process. Facing tight deadlines and hundreds of mission-critical databases, Yext's infrastructure security team could not afford any delays.

Yext Implements Comprehensive Auditing

With 250+ databases that included multiple database types and versions, Yext faced a difficult and potentially costly challenge to implement the comprehensive auditing necessary to pass SOC 2. Yext estimated it could cost over three million dollars without taking into account labor hours to pull off such a large project.

StrongDM enabled Yext to conveniently log every query and permission change without any infrastructure changes. In three weeks, StrongDM was rolled out to hundreds of staff. The ability to produce query and activity logs across Yext's entire infrastructure provided key capabilities that ensured Yext would always be audit-ready.

StrongDM Reduces Provisioning Time from Hours to Minutes

StrongDM offered more than an audit trail. StrongDM's access management streamlined the work to onboard and offboard technical staff, reducing the time to provision access from 48 hours to 30 minutes. This helped transform how the infrastructure team was perceived by peers at Yext. By eliminating frustrating delays, Yext's Infrastructure team was transformed into a business enabler that could empower teams to work more efficiently and securely.

Hearst Simplifies the Deprovisioning Process with StrongDM

HEARST

COMPANY 10

StrongDM Manages Access without Disrupting Productivity

MediaOS acts as the central hub to manage, monitor, and distribute content for Hearst's 21 magazines, including Elle, Cosmopolitan, and Esquire. MediaOS serves content to 150 million readers a month in a latency-sensitive environment. In under two minutes, the MediaOS platform must analyze content to reveal who is seeing what, identify social visitors, and compare that data to that of similar content.

To deliver that performance, the MediaOS engineering team cannot afford any tooling that impacts productivity negatively.

> "You don't even know StrongDM is there. Once it's installed, it just works. It's very simple.
>
> HEARST | Jim Mortko
> *VP of Engineering*

Efficient Access Means Less Work for DevOps

As a critical part of the **Hearst** infrastructure, MediaOS is constantly hiring engineers. Because there are so many services, databases, and developers, the **onboarding and offboarding process** was labor intensive before StrongDM.

Since deploying StrongDM, the process has become much simpler. The DevOps team invites a new hire to the StrongDM platform and assigns a role. The hire inherits all appropriate database permissions. No need to maintain multiple scripts or checklists. That means more efficiency and an easy to access audit trail of every permission change.

StrongDM is Convenient and Secure by Default

Because StrongDM integrates seamlessly with every SQL client, BI tool, and the command line, there's no training required. According to Jim Mortko, VP Engineering, "It's something that you don't even know it's there once it's installed. It just works."

StrongDM is a Dynamic Access Management platform that puts people first by giving technical staff a direct route to the critical infrastructure they need to be their most productive. End users enjoy fast, intuitive, and auditable access to the resources they need. Administrators gain precise controls, eliminating unauthorized and excessive access permissions. IT, Security, DevOps, and Compliance teams can easily answer who did what, where, and when with comprehensive audit logs. It seamlessly and securely integrates with every environment and protocol your team needs, with responsive 24/7 support.