How SaaS Companies Secure Infrastructure Access at Scale

How leading SaaS and technology companies improve security, compliance, and operational efficiency with StrongDM.

strongdm
Now part of Delinea

Table of Contents

Infrastructure Access Challenges for SaaS Platforms

Modern SaaS companies rely on complex infrastructure environments that include cloud platforms, databases, containerized workloads, and internal services. As engineering teams scale, managing secure access to these systems becomes increasingly complex.

Developers require fast and reliable access to infrastructure resources while security teams must maintain visibility, policy enforcement, and control. The organizations featured in this guide demonstrate how SaaS companies modernized infrastructure access while improving security and operational efficiency.

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

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."
>
> coveo™ **Jean-Philippe Lachance**
> *Security Engineering, R&D*

The Limitless Stack Creates Untenable Access Workflows

Coveo Relevance Cloud(TM) 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, Security engineer, R&D 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.”

StrongDM Reduces Administrative Burden of Onboarding

StrongDM also sped up the onboarding process for new hires. Instead of provisioning credentials to each of the hundred databases, Coveo installs the StrongDM console, and employees get one credential to access everything they need.

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

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.

> “
> **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.”**
>
> coveo™ | **Jean-Philippe Lachance**
> *Security Engineering, R&D*

“I need to work on intrusion detection, anomaly detection, AWS account management, hardening those databases, and hardening our AWS resources,” says Jean-Philippe.

Beekeeper Eliminates VPN Pain with Zero Trust Security

BEEKEEPER

Companies around the world use Beekeeper to connect their frontline teams, unify their systems, and drive their businesses forward. Beekeeper's frontline success system helps companies ditch paper and manual processes to improve employee engagement, retention, and performance.

High-growth companies like Beekeeper face a common but fundamental challenge: scaling access management while maintaining security and efficiency. Beekeeper grappled with a complex environment that relied on numerous VPNs–one for every region in AWS and GCP. That meant that engineers had to juggle multiple VPNs, leading to a slow, frustrating experience. Furthermore, every engineer needed credentials to access different endpoints within the network.

The complexity combined with the slow, cumbersome processes inevitably become unmanageable, and Beekeeper knew there was a better world out there.

Why StrongDM Won

Beekeeper did its homework when it came time to enlist an access management partner. The company selected StrongDM after engaging with Teleport and HashiCorp Boundary. According to Head of DevOps Daniel Solsona, StrongDM was the clear winner on the technical front.

Ease-of-Use Leads to Widespread Adoption

Ensuring the right people have the correct privileges if and when they need them is vitally important for the frontline businesses Beekeeper serves, making it critical that any access solution be widely adopted across teams. By being easy to deploy and easy to use, Beekeeper has seen StrongDM deployed and adopted by every team it's been rolled out to.

> "
> **StrongDM was much simpler architecturally than Teleport. With Teleport, you need to run all these different services, and it got to be too much. It was much simpler to run StrongDM compared to Teleport. Hashicorp Boundary was 4-5 years away from what StrongDM is doing now"**
>
> BEEKEEPER | **Daniel Solsona** *Head of DevOps*

Daniel recalls, "The previous approach was nuts and painful, but [StrongDM] is glorious. It's funny; we got lots of people saying, 'This is the best thing that has happened in a long time.' People are loving [StrongDM] because it removes a lot of friction that we had in there before. The ability to onboard and offboard employees has also been greatly simplified. In Daniel's words, the ability to onboard and, more importantly, confidently offboard people by removing a user from the single sign-on (SSO) provider is golden. Now [with StrongDM], we know we just remove the user, and they're gone. We don't have to worry about anything."

Leveraging Access Workflows to Meet the Principle of Least Privilege (PoLP)

When it comes to access requests, Beekeeper uses StrongDM's Access Workflows capability to automate workflows and route human approvals. The ability to make a universal change in the infrastructure (like adding a database in AWS) and have that access extend to whoever needs it in an automated way has been game-changing. There's no need to provision every user or let everyone know a new piece of infrastructure exists.

Now, when an admin makes a change in StrongDM, that change is immediately reflected for all the users in StrongDM. Beekeeper can now easily enable the Principles of Least Privilege (PoLP), granting specific people access only when needed to particular systems in AWS or GCP.

For example, by default, no one in production can access any system containing customer data. Users can, however, request that data through an access workflow and receive read-only access. Admins control when these requests are automated and when they require human approval. By eliminating end-user credentials and leaning into Least Privilege, Beekeeper is on track to achieve its ultimate goal: Zero Trust.

> "
>
> The previous approach was nuts and painful, but [StrongDM] is glorious. It's funny; we got lots of people saying, 'This is the best thing that has happened in a long time.' People are loving [StrongDM] because it removes a lot of friction that we had in there before. The ability to onboard and offboard employees has also been greatly simplified. Now [with StrongDM], we know we just remove the user, and they're gone. We don't have to worry about anything.
>
> BEEKEEPER
>
> **Daniel Solsona**
> *Head of DevOps*

> "
>
> We chose StrongDM for the flexibility and simplicity. Suddenly, achieving Zero Trust is not that daunting because the tools are there. Obviously, you still need to put effort into designing the proper access levels. But you don't need to build anything by yourself. Everything is provided to you."
>
> BEEKEEPER
>
> **Daniel Solsona**
> *Head of DevOps*

Zero Trust Within Reach

This type of dynamic access is the foundation for Beekeeper's Zero Trust initiatives.

Searching for Zero Trust? Discover how StrongDM can transform your organization's access management, ensuring security, efficiency, and scalability. Book a demo.

StackAdapt Simplifies Audits with Total Visibility

StackAdapt is a self-service programmatic advertising platform used by hundreds of brands and agencies around the world. The platform combines machine learning with a clean and intuitive user interface to help media buyers plan, execute, and drive performance across all devices, inventory, and publishing partners. To ensure it could comply with SOC 2 and easily manage access to its infrastructure, StackAdapt implemented StrongDM.

“As a solution for granting access, StrongDM is something that just works. It’s really easy to set up, and the support is great. StrongDM is a product that is getting better and not trying to be too complicated—the product team does a fantastic job of adding features that bring value.” - David Krutsko, Staff Infrastructure Engineer

> "
> When I started, the company had maybe twenty people. We’ve grown to over nine hundred within a couple of years. If we're looking at doubling in size every year, then we need a solution that can handle that growth.”
>
> StackAdapt | David Krutsko
> *Staff Infrastructure Engineer*

Looking to Build at a Scalable Pace

StackAdapt has seen record growth in both revenue and headcount since its inception, and it needed an access management tool that could keep up.

The company had tried another access solution before StrongDM, but it had several significant limitations: Admins couldn’t grant temporary access, and a client needed to be installed on every end resource. These limitations created day-to-day busywork for admins and opened the organization up to risk.

StackAdapt also needed a better way to manage and track credentials. Before StrongDM, the team managed access with multiple point solutions, which limited observability into who had access to what resources. They wanted a unified solution that could manage access across their infrastructure, including databases and websites. Additionally, they needed robust audit logs that captured every query and SSH session.

Low Visibility Meant Lost Opportunities

Before StrongDM, evidence gathering for compliance was tedious and imprecise. The team had to audit databases and SSH access using usernames and passwords. To prove that users had been deprovisioned, admins had to collect screenshots. This process took over an hour, and it was all done manually.

Without visibility into every action on every system, it was difficult to comply with SOC 2—a requirement for many of StackAdapt’s potential customers. This meant lost opportunities to generate revenue for the company in addition to wasted time and effort for the team.

Confident Access Moves StackAdapt Closer to Zero Trust

StrongDM eliminated the need for employees to have access to credentials, moving StackAdapt closer to the Zero Trust security model.

And evidence-gathering for audits is now more consistent and accurate. StackAdapt can generate a report in under a minute and have it cross-checked with their other databases to ensure proper deprovisioning and access auditing. As a result, the team is poised to achieve SOC 2 Type II compliance within months, which positions the organization to unlock bigger deals with enterprise clients.

Best of all, StrongDM makes life easier for the people who use it. It is user-friendly, easy to maintain, and has the ability to grant temporary access to resources. As David Krutsko puts it, “There are surprisingly few tools that can solve this problem for us. StrongDM met our goals and continues to meet our goals. Everyone I speak with right now says it's a great tool and works better than the solutions we used beforehand."

> **"**
>
> **There are surprisingly few tools that can solve this problem for us. StrongDM met our goals and continues to meet our goals. Everyone I speak with right now says it's a great tool and works better than the solutions we used beforehand."**
>
> StackAdapt | David Krutsko
> *Staff Infrastructure Engineer*

Braze Enforces SOC 2 Policies with StrongDM

braze

10,000+	1,500	3
Databases	Servers	Days to deploy

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 used StrongDM to instantly deliver results to our auditors, which really simplified the SOC 2 process.**
>
> braze | 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.

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

Yext Goes Public After Achieving SOC 2 Compliance

250+	$3M+	47 hours
Databases	Annual Savings	Faster to onboard

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.

> "
>
> **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*

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.

Ironclad Shrinks Attack Surface and Onboarding Time using Google Groups Integration

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.

Seismic Centralizes Multi-Cloud Infrastructure Access and Accelerates Growth with StrongDM

Seismic, the global leader in enablement, helps organizations engage customers, enable teams, and ignite revenue growth. The Seismic Enablement Cloud™ is the most powerful, unified enablement platform that equips customer-facing teams with the right skills, content, tools, and insights to grow and win.

Enterprise Acquisitions Introduce Cloud Confusion

From 2019-2021 Seismic experienced exponential growth driven both organically by existing and new customer usage as well as inorganic growth - through strategic business acquisitions. Some of the growing pains they experienced during this time included the fragmentation and expansion of tools, policies, and environments. Each acquisition introduced a new cloud provider, making standardization of access controls and policy management a challenge.

> "
> I've always been impressed with the support team and the engagement at StrongDM. We work with a lot of different vendors (at least 20 or 30). Honestly, I think StrongDM is by far the easiest vendor to interact with from a reliability standpoint, support, and new features that get rolled out."
>
> Seismic
>
> Tom Wojtalewicz
> *Senior Manager Site Reliability Engineering*

Operating in four different clouds (IBM, Azure, AWS, and GCP) introduced significant hurdles in managing access to its diverse infrastructure. Each cloud provider had its specific access management approach, lacking a centralized method to oversee and control permissions. The complexity intensified due to non-standardized permissions across clouds, making it difficult to manage and tailor access to specific groups.

The Need for a Unified RBAC Solution

This complexity prompted the Engineering team to initiate a comprehensive two-year strategy for consolidating and unifying their various environments, with a key focus on finding a more unified Role-Based Access Control (RBAC) solution. The Engineering team recognized the urgent need for more granular controls, particularly in the face of strict security requirements from their customers. The challenges included managing permissions across different clouds (AWS, GCP, Azure), technologies (MS SQL Server, Azure SQL, Postgres, Redis, MongoDB, Kubernetes, etc.), and diverse data store types. The strategy ultimately led Seismic to StrongDM.

Infrastructure Access Centralization and Automation

StrongDM proved to be a game-changer for Seismic, offering secure, centralized, infrastructure access management across its multi-cloud environment. The implementation of StrongDM allowed Seismic to automate access requests and initiate Just-in-Time Access, ensuring that the right individuals received the right access only when needed. This shift helped Seismic achieve the Principle of Least Privilege (PoLP) across all of its critical infrastructure.

Positive User Experience and Collaborative Support

While acknowledging the inevitable initial friction with any change, Seismic found that StrongDM's user-friendly interface and support team made the adoption process smooth and painless. The engagement with StrongDM's support team stood out as one of the best experiences among the various vendors Seismic has interacted with. The ability to work closely with StrongDM engineers to address specific issues, especially in dealing with less mature technologies, reinforced the partnership.

Access Granted in Minutes—Not Days

Seismic even quantified the impact of StrongDM on access management efficiency. Before StrongDM, it could take days to receive access to resources, leading to inefficiencies, user frustration, and manual overhead.

Ian Miller, Principal Site Reliability Engineer, gave this example, "If you have requested access to one service database and that service was deployed in every region that we support, that could easily mean up to 18 different databases for that service and production. So it wasn't always a one-to-one representation in terms of what you got access to. It was hard to keep track of, it was hard to maintain, and it wasn't always clear what that person always had access to."

> "
>
> **...Getting us to a place where we could have Just-in-Time, Least Privileged Access [made all the difference], we really couldn't do it without a solution like StrongDM."**
>
> Seismic
>
> **Tom Wojtalewicz**
> *Senior Manager Site Reliability Engineering*

With StrongDM, the time required for the same process is reduced drastically – down to a matter of minutes. The automation of access requests for resources in AWS and other clouds, especially during onboarding, played a pivotal role in Seismic's ability to scale rapidly and efficiently.

Efficient Access Controls with Zero Security Compromises

As a scaling enterprise, Seismic hosts thousands of customers with strict security and compliance requirements. As an organization, they also operate within compliance frameworks such as SOC 2 and ISO 27001. By leveraging StrongDM's audit logs and session recordings, Seismic's InfoSec, Security, and Privacy teams could also efficiently collaborate in auditing and ensure compliance. "Remaining in compliance and auditing is another benefit. We are able to share data from StrongDM with auditors and show that we have temporary access within our defined limits, with the ability to get more granular by defining roles by geography... Showing that people from this location aren't accessing data from another location." - Tom Wojtalewicz, Senior Manager Site Reliability Engineering

Secure Infrastructure Access: A Firm Foundation for Growth

Seismic faced access challenges from acquisitions and diverse cloud environments which included AWS, GCP and Azure. StrongDM played a pivotal role in automating access management, unifying controls across all cloud infrastructure, and meeting compliance standards. Seismic's adoption of StrongDM has not only addressed immediate access management challenges but has also positioned the organization for sustained growth, scalability, and enhanced security in a rapidly evolving technology landscape.

Common Outcomes For SaaS Companies

Across these organizations, several common outcomes emerged:

- Faster onboarding and offboarding for engineering teams

- Reduced reliance on shared credentials and VPN-based access

- Improved visibility into infrastructure access activity

- Simplified access management across cloud resources

- Better alignment between security and engineering teams

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