Buyers Guide

How to Evangelize a New Access Management System Across Your Enterprise

strongdm

Table of Contents

Introduction

Let's talk about infrastructure access. What do the DMV and modern-day infrastructure access have in common? Both deal with sensitive data, and both are notorious for soul-sucking wait times and tedious piles of paperwork. In the same way, inefficient infrastructure access has become the status quo because it's always been complicated and time-consuming.

How time-consuming? For 57% of organizations, it takes days or weeks for infrastructure access to be approved and granted. In a digital era characterized by automation and instant gratification, the fact that more than HALF of organizations endure excessive wait times to receive access to the databases they need to do their jobs is unacceptable.

But this is how we've always worked. Why should we change it?

The inability to get simple and secure access to critical infrastructure can also tempt teams to resort to insecure practices, such as leaving backdoors open, sharing credentials, and using shadow IT. In fact, 55% of survey respondents report maintaining backdoor access to systems and 53% admit to sharing credentials across teams. This is a common but serious issue with the potential for harsh consequences. While slow access causes headaches for technical staff and damages their productivity, the workarounds can be detrimental to security.

Addressing Infrastructure Access

You want a simple, effective, and secure way to provision and revoke access to infrastructure. Addressing this challenge requires some critical capabilities. These solutions must:

- □ Support any and all technical users–employees and contractors–not just admins.
- □ Connect to everything in the tech stack.
- □ Be secure by design.
- □ Make it easy to report on and audit everything everyone does and when they do it.
- □ Be available to support you when you need help. And when we say available, we mean 24/7 availability, so that when an incident comes along at 1am, you can get in, get it fixed and get back to bed–instead of waiting an hour for access.

Access Management Buyer's Guide

The purpose of this guide is to equip you with the information you need to navigate the purchase process with ease. It will help answer the question: "How do you evangelize a new access management solution into your organization?" It will also help you champion the products and services that work best for your teams and provide actionable outlines for enterprise organizations.

The purchase approval process can be prickly. Finding the right solutions for your team and receiving approval from leadership and procurement to purchase the solution is only half the battle. Nowadays, buying decisions are rarely individual decisions.

According to Gartner, enterprise organizations typically have buying teams of 14-23[1] people who must reach a consensus before moving forward. Veteran buyers agree that the second half of the battle is convincing others within your organization of what you already know (the problem and how to fix it) and gaining their support. Fortunately, there are steps you can take to make the task as smooth as possible.

The Buying Process

What to expect

If you're reading this guide, chances are you already understand the challenges your team faces, as well as the benefits of addressing them. If you have that defined, the next step is to identify the list of internal stakeholders who must approve the purchase and prepare to answer the questions that will inevitably come your way.

Questions to consider before starting the process:

- How are things working now?
- What's wrong with how things are working?
- How would you like things to be?
- How will your organization benefit if you make improvements?
  And, the corollary: How will you be negatively impacted if you don't?
- What's required to bridge the gap?

[1] Barnes, H., Egloff, D., & Marino, M. (2021). Focus on Buying Jobs Rather Than the Chaos of Buying Journeys. Gartner. https://doi.org/G00761241

Building the business case

The best place to start your buying process is with the business case. This will help you answer critical questions regarding the need, the investment, and the expected outcomes. Most business cases lead with one of three primary objectives: reduce risk, cut costs, or increase revenue. These objectives will be important to the buying team and create a framework for making purchases with impact.

There is a set of tangible steps in this process. These steps define the problem and expected benefits before any mention of needed technology or specific products. They outline the problem statement, the benefits of addressing the problem, and who you'll need to work with to drive the project forward.

These include:

- Document the pain
- Define project goals
- Define expected benefits
- Understand your organization's process
- Identify stakeholders
- Align on use cases to be addressed

Once the above is complete, you'll be prepared to have conversations about your organization's challenges, why they're worth addressing, and how to solve them. This is when the conversation about tools and technologies begins—how can a new tool help solve the problem? With your business case prepared, a strong technology partner should be able to help you:

- Propose a solution to the problem
- Prepare the necessary demos/proofs-of-value needed for all your internal stakeholders
- Partner with your economic buyer to drive or purchase through your internal processes

Document the pain

Chances are you already know where the pains are, and you're on the path to resolving them. The problem? Other stakeholders in the buying process may not share or even be aware that the pain exists.

That's why the first step is to document the pain. This will enable you to clearly articulate where the issues are and why this is a problem worth addressing. Documenting the pain will be especially important as you begin to work with an economic buyer or with procurement on a particular purchase.

There are different ways you can define the pain for your stakeholders. If possible, a mix of all approaches is ideal, as different stakeholders will have different priorities and requirements to approve a purchase.

Approach	Description	Example
Quantitative	Ability to quantify the pain in terms of hours, costs, etc.	Every access request takes, on average, 5 days to be approved. That means our engineers spend roughly 40 hours waiting for each access request to be approved.
Qualitative	Description of the pain in terms of daily activities and impact to the organization.	The inability to have simple and easy access to the tools we need to do our jobs results in missed deadlines and delayed projects.
Anecdotal	Quotes or feedback from others in your organization internally that qualify the pain felt.	"Waiting for access basically brings my work to a halt until it's provided. I'd be more productive if I could just get access to the systems I need, when I need it." -Emily Engineer, Sr. Engineer

The intent here is to clearly explain the pain the organization feels in order to justify a potential purchase of a tool to address it. The next step is to define the project's goals and the expected benefits of resolving this pain.

Defining key outcomes is a critical step in defining the business case. These outcomes represent, and often quantify, the benefits that your team can expect to receive from deploying a product.

Define project goals

Below are some example questions you can use to build the initial business case. While not every question applies to every organization, being able to answer these questions (estimates work) will streamline conversations and expedite the process.

Goal: Protect the Business

- How much time does it take to add new technologies to access/security policies?
- On average, what is the number of exceptions made to security policy?
- Exactly how many users have admin/root access?
- Do you have a plan for getting visibility into user actions on every system?
- How many passwords/secrets do the technical staff use?

Goal: Improve Productivity

- What is your goal for reduced (reallocated) IT spend–e.g., VPN, legacy PAM, labor?
- On average, how much time do you spend managing access or waiting to receive access (including onboarding new hires and managing time-bound access)?
- How much time do you spend collecting evidence for audits and/or investigations?
- How much time do you spend servicing the lifecycle of users–joiners, movers, and leavers?
- How long does it take your team to complete deployment of the access solution?

Goal: Grow, Scale, Enable the Business

- What is the number of shared credentials across your stack?
- What is your ideal time to complete deployment of an access solution?
- What do your MTTI (Mean-Time-to-Investigate) and MTTR (Mean-Time-to-Response) numbers look like? Where do you want them to be?

Define expected benefits

Once you've clearly identified and documented the problem that the solution is intended to address, the next step is to define the expected benefits of addressing the problem. One of the most impactful methods of demonstrating the benefits is to spell out your current state, the challenges to that approach, and the expected future state. See below for an example.

	Before Environment	Common Setbacks	Future State with StrongDM
Protect the Business Apply least privilege access and observability across your entire infrastructure	• Credentials are difficult to manage and track • Users are given too much or too little access • Complexity in existing processes causes workarounds • Corporate identity does not apply to all systems	• Failed compliance audits; investigations are difficult • Proliferation of credentials lead to increased risk/ exposed security gaps • Diminished brand reputation and/or financial impact of security breach • Frustrated employees circumvent security policies increasing risk and causing compliance drift • Overly permissive access leads to data privacy violations	• The right people have the right access at the right time • Eliminated gaps in infrastructure access observability • Reduced attack surface because you never expose credentials or network segments • Ability to complete access audits more accurately and efficiently • Increased cooperation between tech teams (engineering, IAM, security, compliance, IT)

	Before Environment	Common Setbacks	Future State with StrongDM
Improve Productivity Enable staff to do more high value work with less waiting, fewer manual tasks	• Administrators spend too much time provisioning and deprovisioning access to infrastructure • Technical staff wait too long for access • Implementing access controls for security and compliance takes too long • Collecting access evidence for audits takes too long • Technical staff are frustrated and work inefficiently	• Missed project deadlines • Increased employee churn • Time spent waiting instead of working • Time spent doing low-value manual provisioning tasks • Cannot adopt new technologies because of time spent supporting legacy access methods • Audits take too long and are messy	• Simplify infrastructure access—easy to manage and use • Employees are empowered to do their work • Maximize focus on strategic initiatives • Faster answers to who did what, when, and where for auditing and compliance • Increased cooperation between tech teams (engineering, IAM, security, compliance, IT)
Grow, Scale, Enable the Business Accelerate the secure and compliant adoption of modern technologies	• Unable to build at a scalable pace • Unable to confidently overcome security objections • Not compliant and the operational burden to get compliant is too large or it is a distraction • Complexity in existing processes causes shadow IT • No visibility into what's in the stack or who has access • Unable to deploy new technologies because legacy access management won't support them	• Limited opportunity to generate revenue: lost / contracted market share, competition, differentiation • Lost revenue due to security objections from prospects • Financial loss and damaged brand reputation due to breaches • Increased employee churn: losing best people, difficult to recruit top talent • Wasted time and effort during audits	• Technical staff complies with security systems and policies • Increased focus on your core product instead of building internal access solutions • Crisp answers to access control questions, confidence to overcome security objections to win deals • Completing access audits is less stressful and more efficient • The tech stack accelerates the business

Understand your organization’s purchasing process

Understanding the process your organization uses for purchases and procurement upfront can save you from major headaches later in the purchasing process. For example, if your organization requires that every tool be SOC 2 compliant, and if your chosen vendor is not compliant, you may need to stop and reevaluate your options.

Below are a few questions that will help you understand the purchasing process in your organization.

What is the paper process?

This includes contractual documents, NDAs, and any signatures required to formalize a deal as well as legal, financial, and purchasing resources.

What does the decision process look like?

The decision process will lay out how you will evaluate, select, and purchase a solution.

Are there any compliance requirements that must be met?

Defining the security and compliance requirements upfront can prevent you from getting further down the path and hitting a roadblock.

Who needs to approve and sign off on the purchase?

This will help you with the next step—clearly identifying who needs to be involved in the process whether that’s someone from exec staff, procurement, or IT.

Identify your stakeholders

In addition to understanding the steps it takes to successfully purchase a product, you also have to know who will be involved, how long it could take, and who could say no. Additionally, you must be able to prove how this purchase will result in positive business outcomes for your organization.

The buying team you’ll work with to complete the purchase will differ depending on your organization and the processes involved. Furthermore, each organization will have its own set of priorities and require different things from solution providers. Appeasing everyone isn’t always possible, but understanding each group will help the buying process move more smoothly and efficiently.

While there is some overlap between stakeholders and users or buyers, there are also new players who join at later stages in the process. Ensuring alignment across all stakeholder groups is critical for the purchase and adoption of solutions. Creating a simple table is one of the best ways to track and understand each team, the team's role, and what the team cares about. Here is an example:

Team	Team Members	Requirements
Engineering		
IT		
Etc.		

Align on use cases to be addressed

Understanding common use cases is one of the most important steps in the buying process. Use cases show buyers how the solution has been utilized in the past and explain the key outcomes.

Below is a list of use cases for privileged access management. These will help to clearly define how a potential product will be used, and the outcome you can expect.

Use Case	Outcome
Permission Management	Every access request takes, on average, 5 days to be approved. That means our engineers spend roughly 40 hours waiting for each access request to be approved.
Session Management	Grants elevated permissions only to certain tasks or functions—a more granular approach to privilege escalation than PAM tools.
Just-in-Time Access	Ensures that every technical employee receives only the access they need, when they need it. Revoking access is automated now, so it won't hold your technical staff back. Get time back to work on high-value projects.
Vendor Access	Achieve peace of mind knowing you can grant vendors just-in-time access with an audit trail of every query and command.
Privileged Credential and Secrets Management	Manage, store, and retrieve secrets like passwords, tokens, and keys for software and infrastructure resources.
Logging and Reporting	More detail, more answers, and faster coverage with automatic evidence collection.
Security Standards and Frameworks	Easily implement security policies for access control with granular access control and comprehensive audit logs.
Privileged Access Management for the Cloud	Manage privilege access from one central control plane whether you have a multi-cloud or hybrid environment.

Build support for your preferred tool

Once there's agreement that a problem exists and needs to be addressed, the next step is to begin discussing approaches that can resolve that pain. This will often be discussed in terms of technology, tools, and processes.

When it comes to technology and solution providers, there are a few key questions that you should be prepared to answer upfront:

- ✓ **Does this solution provider have proof of tangible business benefits that are relevant to your most important business goals?**
  For example, are there customer case studies available for your chosen vendor? Having these in your back pocket will help you with the executive-level and procurement process, as these stakeholders will often want to see how similar companies have addressed the problem with your chosen vendor. Furthermore, case studies will help you validate that your chosen vendor is a safe bet, as they have seen success at similar companies.

- ✓ **What are the decision criteria that will be used?**
  This question shows that you have outlined the key capabilities a tool must have to adequately solve the pain and support your expected outcomes. We dive deeper into this below.

- ✓ **What strengths, weaknesses, and differentiators do competitors have? Are you ready to defend one solution over another?**
  Some organizations require that departments evaluate multiple tools for every purchase. Understanding the landscape and each vendor will prepare you to answer any questions regarding other potential solutions.

Having clear answers to these questions will help ease the buying process. Furthermore, the answers will show that there is a defined set of criteria a potential vendor must meet to solve the problem.

Define the decision criteria

Defining the criteria to be used in your purchase is one of the most important steps in the purchasing process, as these criteria will be used to decide which vendor will be selected. Decision criteria can range from specific features to intangibles such as industry analyst references, customer support, or deployment timelines.

When it comes to privilege access management, below are some common criteria that are often used in purchasing decisions.

Critical Capability	Criteria
Precise Control	Admins must have precise control over what each user has access to—without these controls ever getting in the way of productivity.
Total Visibility	You must have total visibility into everything that's ever happened in your stack. This enables security, compliance, and auditing teams to easily answer who did what, where, and when.
Secure by Design	Security is a first-tier consideration in product design. Unauthorized access is eliminated because users never see resources they don't have permission to use.
Confident Access	Clear, direct, and auditable paths provide individualized access to the right people so admins are more confident and faster to say 'yes.'
Works with Everything in the Modern Stack	All past, present, and future infrastructure tooling decisions will always be supported.
Superior User Experience	User experience considerations extend beyond security and admin teams to the end users, making the product simple and easy to adopt. Every team member has a clear path to what they need—when they need it.
Exceptional Customer Support	The chosen vendor is a strategic partner in your security strategy, providing responsive and available customer support. That means every support engineer is also a practitioner.

Conclusion

Infrastructure access requirements have changed drastically over time. It's no longer enough to focus on privileged accounts or prioritize web applications. Picking the right vendor and partner is critical to ensuring that your organization can meet these new requirements and adapt as future ones appear. This document will give you a starting point to identify the gaps, drive those discussions, and ultimately adopt a vendor that will support you through this process. For more information, or to get started on this journey, please visit **www.strongdm.com.**

Vendor Example: StrongDM

StrongDM Overview

StrongDM is a proxy that combines authentication, authorization, networking, and observability into a single product. The product is designed to unify and simplify infrastructure access workflows by providing low-friction connectivity to virtually every piece of infrastructure in your stack. This approach has some key benefits, depending on your role in the organization:

- **DevOps:** Teams can provision and deprovision access to specific instances, servers, or databases in a matter of clicks.
- **Security & Compliance:** Teams can gain full visibility into "who did what when" on each system and see when individual users have executed on specific systems. For compliance, full records are kept of "who was in each system and what were they doing" at any given point in time.
- **Admins:** Grant and revoke access to critical infrastructure quickly and easily, greatly simplifying user onboarding and offboarding, provisioning for third parties, and enabling access for a specified period of time. Users, roles, and access are easily managed via an Admin UI (CLI available as well).

Requirements:

- ✓ Capable of supporting any and all technical users—employees and contractors—not just admins.
- ✓ Capable of connecting to everything in the tech stack.
- ✓ Secure by design.
- ✓ Easy to report on and audit everything everyone does—when they do it.
- ✓ 24/7 availability.

Critical Capability	Criteria	StrongDM
Precise Control	Admins must have precise control over what each user has access to—without these controls ever getting in the way of productivity.	✓
Total Visibility	You must have total visibility into everything that's ever happened in your stack. This enables security, compliance, and auditing teams to easily answer who did what, where, and when.	✓

Critical Capability	Criteria	StrongDM
Secure by Design	Security is a first-tier consideration in product design. Unauthorized access is eliminated because users never see resources they don't have permission to use.	✓
Confident Access	Clear, direct, and auditable paths provide individualized access to the right people so admins are more confident and faster to say 'yes.'	✓
Works with Everything in the Modern Stack	All past, present, and future infrastructure tooling decisions will always be supported.	✓
Superior User Experience	User experience considerations extend beyond security and admin teams to the end users, making the product simple and easy to adopt. Every team member has a clear path to what they need—when they need it.	✓
Exceptional Customer Support	The chosen vendor is a strategic partner in your security strategy, providing responsive and available customer support. That means every support engineer is also a practitioner.	✓

Additional Features

- ✓ Speed. Connect in minutes, not hours.
- ✓ Grant/revoke access instantly.
- ✓ Audit logs are comprehensive and fully automated.
- ✓ Usability. Simpler, faster, more intuitive workloads.
- ✓ Faster time to value with simple deployment and an agentless architecture.
- ✓ Exceptional customer support.
- ✓ People-First mentality to business operations and support.
- ✓ Total visibility into every action and system.
- ✓ Secure by design. Credential-less access never exposes passwords to users.
- ✓ Natively supports a large breadth of protocols and resources across the modern tech stack.

StrongDM: Customer Validation

Olive AI: Seamless Access & Elevated Data Layer Security

Industry

Healthcare

Challenges

Inefficient Access Patterns: When Olive launched, the company primarily managed database access with Ansible. Access to customer systems (RDP into Windows server) required connecting to Olive's corporate VPN and then RDPing into a server via a business-to-business (B2B) VPN tunnel. The team audited data access via time-consuming custom scripts, usually written in Bash or Python.

Lack of Visibility: 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. Provisioning VPN accounts for one-off database access requests caused headaches for the IT team.

Outcomes Achieved with StrongDM

- Standardized Access Control Patterns: StrongDM supported Olive's entire stack, including RDS, Redshift, DynamoDB, Athena, and RDP access to customer systems. The team no longer has to create one-off users for each database. StrongDM enabled Olive to standardize its access control patterns.

- Seamless Access for End Users: StrongDM has made it possible to get developers onboarded and working on day one, and ensures they all have a single, standard login with access to all the infrastructure they need.

- High Level Security and Compliance: Olive no longer has users in its data layer, which is ahead of most regulatory requirements. StrongDM also provides a line-by-line, high-fidelity audit trail of access to core databases.

> "
>
> **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*

StrongDM on G2

★★★★★ Feb 22, 2022

"Minimal Overhead, Maximum Value"

What do you like best about strongDM?

StrongDM has minimal overhead to run. Setting up in k8s is a breeze, and has a boilerplate template in the documentation with configuration needed.

We honestly didn't need to compare to the competion because how quick it was to install and configure.

★★★★★ June 09, 2022

"Amazing product with a great team"

What do you like best about strongDM?

StrongDM's product is extremely intuitive and powerful. We use it to manage remote access to customer sites; auditing and RBAC are crucial for our use case, and these features are baked right into the product and are easy to use. We can set up approval workflows using AccessBot's native features or custom workflows using the API. Everyone at the company that we've worked with Sales, Customer Success, and Support – is passionate about the product and great to work with. I would recommend strongDM, both as a product and a company, to anyone looking to secure access to their infrastructure.

★★★★★ June 09, 2022

"Easy and secure unified access control"

What do you like best about strongDM?

StrongDM unified our access methods across a variety of production instances, gave us more granular control over that access, and simplified the process for the dev team. It's rare to see a product that improves security and usability at the same time.

★★★★½ May 17, 2022

"Easy and secure unified access control"

What do you like best about strongDM?

I like that StrongDM makes it easy for our users to securely access cloud resources without needing a separate VPN. We can provide SSH access to instance, access to databases, and even dashboards for tools that we don't want to make publicly available. Additionally. StrongDM allows us granular control over the resources that individual uders have access to. StrongDM support is also fantastic. Any time we have had issues, they have been able to get us a resolution faster than I would have expected.

What do you dislike about strongDM?

They isn't anything that dislike about StrongDM. We have been a customer for several years now and have seen the product continually improve throughout the time we've used it. I can't wait to see what they come up with next.

Template: Building The Business Case

- □ Document the pain
- □ Define project goals
- □ Outline expected benefits
- □ Understand your organization’s process
- □ Identify stakeholders
- □ Align on use cases to address

Document the pain

Question	Answer
How are things working now?	
What’s wrong with how things are working?	
How would you like things to be?	
How will your organization benefit if you make improvements? And, the corollary, how will you be negatively impacted if you don’t?	
What’s required to bridge the gap?	

Document the goals

Goal: Protect the Business

Question	Current	Goal
On average, what is the number of exceptions made to security policy?		
Exactly how many users have admin/root access?		
Do you have a plan for coverage of visibility into user actions on every system?		
Is there an agreed upon number of error-prone steps to deploy and operate solutions?		
How many passwords/secrets do the technical staff have?		

Goal: Improve Productivity

Question	Current	Goal
What is your goal for reduced (reallocated) IT spend—e.g., VPN, legacy PAM, labor?		
On average, how much time is spent managing access or waiting to receive access–including just-in-time access and new hire onboarding?		
How much time is currently spent collecting evidence for audits and/or investigations?		
How much time is spent servicing the lifecycle of users–joiners, movers, leavers?		
How long does it take your team to complete deployment of the access solution?		

Goal: Grow, Scale, Enable the Business

Question	Current	Goal
What is the number of shared credentials across your stack?		
What is your ideal time to complete deployment of an access solution?		
What do your MTTI (Mean-Time-to-Investigate) and MTTR (Mean-Time-to-Response) numbers look like? Where do you want them to be?		

Define expected benefits

Before Environment	Common Setbacks	Future State
Protect the Business Apply least privilege access and observability across your entire infrastructure		
Improve Productivity Enable staff to do more high-value work–less waiting, fewer manual tasks		
Grow, Scale, Enable the Business Accelerate the secure & compliant adoption of modern technologies		

Identify stakeholders

Team	Who They Are	What They Do
IAM/SSO User		
Security User		
DevOps or SRE Group User		
IT User		
Engineering User		
Engineering Leadership User		
Executive Sponsor or Economic Buyer		

Align on use cases

Use Case Examples	Outcome
Permission Management	Allows users to have full administrative access for a limited period of time, which is monitored and logged.
Session Management	Grants elevated permissions only to certain tasks or functions—a more granular approach to privilege escalation than PAM tools
Just-in-Time Access	Ensure that every technical employee receives only the access they need, when they need it. Revoking access is automated now, so it won't hold your technical staff back. Get time back to work on high-value projects.
Vendor Access	Achieve peace of mind knowing you can grant vendors just-in-time access with an audit trail of every query and command.
Privileged Credential and Secrets Management	Manages, stores, and retrieves secrets like passwords, tokens, and keys for software and infrastructure resources.
Logging and Reporting	More detail, more answers, and faster coverage since evidence collection is automated.
Security Standards and Frameworks	Easily implement security policies for access control with granular access control and comprehensive audit logs.
Privileged Access Management for the Cloud	Manage privilege access from one central plane whether you have a multi-cloud or hybrid environment.

Align on use cases

Use Case	Outcome

Key Questions To Ask While Vetting Prospective Solution Providers

Asking the right questions during the vetting process will help you fully understand the offerings and limitations of each vendor.

1. What does the support model look like?
2. Who are the key stakeholders as it relates to account management? AE vs sales engineer vs CSM? Who do we "get" at our disposal?
3. Who has access to our information and at what level? Day-to-day or break-glass scenarios?
4. If there's an outage, how do you react to that and in what timeframe?
5. How do we compare to other vendors in this space?
6. What is the future state? What is on the roadmap?
7. How do you support customers with their technology stack?
8. What does deployment look like?
9. How much time will this vendor save us each month?

Comparison Checklist

Feature Type	Feature	StrongDM	Vendor 2	Vendor 3
Deployment	No install required on your servers	✓		
AuthN	Credential leasing	✓		
AuthN	OIDC support	✓		
AuthN	SAML support	✓		
AuthN	Authentication thru SSO	✓		
AuthN	MFA integration	✓		
AuthZ	User & group syncing with IdP	✓		
AuthZ	User & group provisioning thru IdP	✓		
AuthZ	ABAC	✓		
AuthZ	RBAC	✓		
AuthZ	Temporary Access	✓		
AuthZ	Protected access to databases	✓		
AuthZ	Protected access to SSH	✓		
AuthZ	Protected access to RDP	✓		
AuthZ	Protected access to Kubernetes	✓		
AuthZ	Protected access to cloud accounts	✓		
AuthZ	Protected access to web apps	✓		
Audit	Database audit logs	✓		
Audit	SSH audit logs & session replays	✓		
Audit	RDP audit logs & session replays	✓		
Audit	Kubernetes audit logs & session replays	✓		

Comparison Checklist

Feature Type	Feature	StrongDM	Vendor 2	Vendor 3
Audit	Cloud audit logs	✓		
Audit	Web audit logs	✓		
Audit	Encryption keys (customer-owned)	✓		
Audit	Secure log storage	✓		
Audit	Log export to SIEM	✓		
Certification	SOC 2	✓		
Certification	FedRAMP	✗		
Support	24/7/365 support	✓		
General	Open source	✗		
General	Pricing	Monthly per seat Unlimited tools included		

strongdm

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.