

aws marketplace

StrongDM

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 12

Other Solutions Considered..... 13 - 15

ROI..... 16 - 17

Use Case..... 18 - 23

Setup..... 24 - 25

Customer Service and Support..... 26 - 27

Other Advice..... 28 - 33

Trends..... 34 - 35

About PeerSpot..... 36 - 37

Product Recap



StrongDM

StrongDM Recap

StrongDM streamlines secure, password-less access, reducing attack surfaces with its zero trust approach. It integrates smoothly with existing systems supporting IP whitelisting and excels in managing runtime features while offering comprehensive audit logging and seamless resource access.

StrongDM provides organizations with enhanced security through features like password rotation and efficient management of access to resources such as EC2 instances, Kubernetes clusters, and databases. Its integration capabilities are complemented by cost-effectiveness compared to competitors like CyberArk. Companies utilize StrongDM for controlling access in dynamic environments, benefiting from audit logging for detailed movement tracking. While users appreciate its efficiency, they also seek improvements in update control and better accompanying documentation. Some express the need for a cloud-native option to address diverse demands, as the current setup can be challenging without comprehensive materials. Flexibility and more traditional PAM features are in demand.

What are StrongDM's key features?

- **Secure Password-less Access:** Facilitates client connections without passwords to reduce attack vectors.
- **Zero Trust Architecture:** Maintains stringent security protocols with a zero trust approach.
- **Seamless Resource Integration:** Works effectively with systems like EC2 and Kubernetes clusters.
- **IP Whitelisting Support:** Enhances third-party resource accessibility with targeted IP controls.
- **Audit Logging:** Provides detailed tracking of user interactions within systems.
- **Password Rotation:** Regularly updates access credentials to boost security.

Why is StrongDM beneficial in reviews?

- **Cost-Effectiveness:** Competitive pricing offers value against alternatives.
- **Resource Management Efficiency:** Simplifies access to complex systems.
- **Enhanced Security:** Protective measures reduce vulnerabilities and ensure secure transactions.
- **Zero Trust Implementation:** Adopts advanced security models right into client operations.
- **Operational Streamlining:** Eases the access management process for multiple environments.

In industries managing sensitive data or requiring regulated access, StrongDM is crucial for securing cloud private networks and managing user access to databases and hosts. DevOps

teams benefit from its ability to protect connectivity to backend servers, ensuring identity and access management remains robust and adaptable for companies dealing with frequent changes or expansions.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “By adopting StrongDM, we have achieved benefits such as eliminating our weekend outages, streamlining ongoing on-call workflows, enabling seamless migration with POC transitions directly into production with minimal effort, allowing our engineers to use their preferred SQL clients like MySQL, PostgreSQL, and Workbench, and facilitating compliance through detailed session logs and query capture for SOC 2 and ISO audits.”



Amit Rathod

Senior Analyst at Toll Holdings Limited

- ✓ “StrongDM positively impacts our organization in many ways, mainly in cost savings from the time saved, and it has significantly improved both security and operational efficiency for us.”



Mohit X

Dev Ops Engineer And Solution Architect at Scania

- ✓ “Since using StrongDM, I estimate around a 60% reduction in effort compared to other PAM tools.”



Verified user

Senior Solution Advisor at a tech vendor with 10,001+ employees

- ✓ “StrongDM has positively impacted my organization by saving me a lot of time as a security auditor, because I have to navigate settings and configurations to check the presence of certain security controls in place.”



Verified user

Solution Delivery Advisor at a tech vendor with 10,001+ employees

- ✓ “The best features in StrongDM are the password rotation capabilities, which I think are pretty cool, and also how you can literally log in to any of the privileged servers through a single platform.”



Verified user

Iam Engineer at a manufacturing company with 10,001+ employees

- ✓ “I absolutely would say that the best features of StrongDM and what I appreciate about the solution is that time to onboard is absolutely minimal.”



Vlad Gust

Director at LivePerson

- ✓ “The best features in StrongDM are that it is the easiest product in the market for this situation with easy access.”



Ibrahim Hassan Barakat

Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

What users had to say about valuable features:

“The best features that StrongDM offers include centralized access management, which I would say is the best feature provided.

“Centralized access management helps me by giving users access all in one place where they can easily access resources such as databases, internal applications, and VPN access. All of these resources can be managed at one centralized platform, giving unified access to users. Centralized access management is something I appreciate about StrongDM..”

Verified user

Associate Software Engineer at a computer software company with 201-500 employees

[Read full review](#) 

“The best feature StrongDM offers is that it is easy to integrate with a command line.

The command line integration helps me in my day-to-day work because our DevOps team created a script that automatically connects StrongDM to the correct cloud resource, and it works all the time.

I find the ability to integrate StrongDM via command line and UI that allows me to connect or disconnect specific resources useful and unique; the ease of it stands out for me.

StrongDM has positively impacted my organization by ensuring that every developer has access to cloud resources, which are audited by the organization, allowing us to keep track of who accesses what and control the access..”

Dmitry Ginsburg

Principal Software Engineer at a tech vendor with 1,001-5,000 employees

[Read full review](#) 

“The best features that StrongDM offers include a proxy-based system that aids in Just-In-Time access, ultimately helping to remove long-standing access, which every organization looks for to reduce high privilege accounts. Every user gets access based on their required need.

StrongDM has impacted my organization positively by being user-friendly with automation and command-line utilities, which have reduced effort. Customers can access it via browser or client, offering many options for utilization.

StrongDM's ability to unify access across different systems is significant; it allows for individual resource mapping and ensures users can connect through appropriate proxy clusters for target machines.

I see the importance of StrongDM's continuous authorization as having periodic checks enabled by identity governance tools, ensuring that access is necessary for a certain period according to access review processes..”

Verified user

Senior Solution Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

“The best features StrongDM offers include the JIT access and workflows, which is the Just-in-Time access provided by StrongDM. Apart from that, there are features like the context-aware policy engine, which helps this tool integrate with endpoint security providers like CrowdStrike and SentinelOne. It also offers comprehensive session visibility and auditing, which helps in session recording and captures all the SSH and RDP terminal sessions as replayable video files. Additionally, it has the ability to navigate with SIEM tools, such as Splunk or DataDog, used to capture all the logs of the servers or cloud storage tools such as Amazon S3 bucket or EC2 instances. Those features are very handy and can integrate very easily with StrongDM. It also offers infrastructure-wide protocol support, whether it talks about PostgreSQL, MySQL, or any database tool. It has secrets management and offers a secret vault agnostic feature through which it can be integrated with any encryption key management tool such as HashiCorp or AWS Secrets Manager. The best thing about it is that it offers a developer-friendly deployment, which is very straightforward and simple with StrongDM PAM tool.

“StrongDM has positively impacted my organization by saving me a lot of time as a security auditor, because I have to navigate settings and configurations to check the presence of certain security controls in place. When I am auditing StrongDM, it obviously helps me. It has a very user-friendly UI, with which any auditor or any security professional will find it easier to navigate different options to check the presence of security controls. Apart from that, it also offers dynamic access control, enforcing restrictions based on user role, time of the day, location, and device context. These features help auditors significantly..”

Verified user[Read full review](#) 

Solution Delivery Advisor at a tech vendor with 10,001+ employees

“I find several best features in StrongDM, but our primary use case focuses on ensuring that we do not have long-lived credentials. The best features for us are the centralized access control and the detailed audit logging, which allow us to provide temporary privileged access without managing VPNs ourselves. I appreciate how well it integrates with Kubernetes and cloud environments on AWS. A significant advantage was simplifying onboarding and offboarding processes, taking away a lot of time and minimizing the risk of overlooking these tasks.

“The audit logging feature significantly helps my team during troubleshooting and internal security reviews. With multiple teams accessing Kubernetes clusters in our production environments, it provides clear visibility into who accessed what and when. While we could use CloudTrail, fetching details from it requires complex SQL queries, making it challenging. StrongDM simplifies this, reducing manual tracking efforts and improving accountability, especially important for compliance with specific regulations we need to follow.

“StrongDM positively impacts our organization in many ways, mainly in cost savings from the time saved. It has significantly improved both security and operational efficiency for us. Previously, access management across AWS and Kubernetes was manual and highly coordinated, relying on VPNs. With StrongDM, onboarding and temporary privileged access processes became much faster and more standardized, enhancing our security posture while maintaining necessary compliance..”

Mohit X

Dev Ops Engineer And Solution Architect at Scania

[Read full review](#) 

StrongDM connects a user to a database or server, but once the session is established, it treats the runtime as a black box and cannot natively enforce fine-grained or attribute-based access control, such as restricting raw column visibility. For a generic TCP resource, StrongDM only records metadata — who, when, and what — instead of capturing the actual commands or payloads executed within the session.

StrongDM's continuous authorization is important for our organization; its scalability, role-based access management, and robust audit capabilities enable us to automate access workflows, retire shared SSH keys, and enhance security. Developers gain self-service access to scrubbed, production-like databases, simplifying testing and development. This is a great feature.

“Our impression of StrongDM's credential-less access control and its integration with existing vaults and secret managers is positive. We are integrated with AWS, have an integration team that captures all the configuration, and have added their process, exposing sensitive data while our AI agents help configure these things automatically, making it very easy to deploy.

“StrongDM unifies access across different systems in our organization by providing various policies that can trigger step-up multi-factor authentications or automated manager approvals when a user attempts to execute a risky operation. It builds and handles non-deterministic AI agents, logging every query, keystroke, and response to provide complete, searchable records satisfying compliance and governance. Whenever our engineers need access, administrators or our team admin can remove their standing access entirely, and users can request temporary access for a defined period via the StrongDM portal or apps like Slack, which automatically expires once the time limit is reached. .”

AmitRathod

Senior Analyst at Toll Holdings Limited

[Read full review](#) 

Other Solutions Considered

“Before choosing StrongDM, I evaluated it alongside other options such as HashiCorp. StrongDM has proven to be comparatively better, despite some feature gaps..”

Verified user

Senior Solution Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

In comparing StrongDM with other solutions, the only other points of reference I have are CyberArk and SailPoint. SailPoint is not a PAM solution, so we will not include that. Compared to CyberArk, StrongDM is far more modern. It is far less clunky. It requires less maintenance of infrastructure. I would say it is plain better. I am also very biased against CyberArk because I absolutely dislike that product.

Vlad Gust

Director at LivePerson

[Read full review](#) 

“Before StrongDM, we explored different options but primarily relied on traditional VPN access and manual SSH key management, along with some AWS native workflows. Those methods worked initially but as our Kubernetes clusters expanded, they proved difficult to maintain consistently across teams, prompting us to seek alternative centralized access solutions..”

Mohit X

Dev Ops Engineer And Solution Architect at Scania

[Read full review](#) 

“There are no challenges because I already had knowledge in this area from using similar types of products other than StrongDM. The unique approach that StrongDM offers is centralized access where I can provide user access to all types of resources such as internal applications, which could be databases or Kubernetes clusters. This is one of the features that StrongDM has, and it represents the unique value and the approach I have experienced while using StrongDM..”

Verified user

Associate Software Engineer at a computer software company with 201-500 employees

[Read full review](#) 

“I evaluated other options, including Teleport for centralized access management and AWS native tools like Session Manager and CloudShell using AWS Vaults. However, they were mainly services without the complete product offerings needed at an enterprise level. StrongDM distinguished itself by providing a simpler user experience, robust auditability, and alignment with our enterprise requirements..”

Mohit X

Dev Ops Engineer And Solution Architect at Scania

[Read full review](#) 

I have evaluated other options including Teleport, a strong competitor to StrongDM, but we chose StrongDM for its completeness of offering in terms of identity lifecycle management and context-based policies, not requiring installation on servers, providing multiple and concurrent vault support, very high availability, a high rate for disaster recovery, and actionable reporting. StrongDM provides greater features for unused privileged access, sensitive resource agents' access, and access reviews in terms of security.

I would recommend using StrongDM when comparing it to Teleport because it provides features including completeness of offering, lifecycle management, and context-based policies, along with great ease of use in installation and multiple vault support. I encourage other clients to choose StrongDM over Teleport. .”

AmitRathod

Senior Analyst at Toll Holdings Limited

[Read full review](#) 

ROI

Real user quotes about their ROI:

We need fewer employees now because StrongDM saves our time by eliminating manual work. While it is costly, the return on investment for this product is good overall.

AmitRathod

Senior Analyst at Toll Holdings Limited

[Read full review](#) 

When it comes to return on investment, questions of that nature are really difficult to quantify. I have not done a dollar to time saved assessment. I can definitely say that it saved us time, and a lot of it. Probably months worth of time in engineering and IT support. Return of investment in two years, we perhaps broke even.

Vlad Gust

Director at LivePerson

[Read full review](#) 

“I have definitely observed a return on investment through the operational efficiency gains and streamlined access management. The onboarding of temporary privileged access accelerated significantly, allowing us to release consultants much faster than before, saving considerable money. We also reduced reliance on manual VPN workflows, cutting high network costs linked to repetitive approval processes. While it is challenging to quantify with a single figure, the time savings and reduced operational overhead were certainly impactful..”

Mohit X

Dev Ops Engineer And Solution Architect at Scania

[Read full review](#) 

Use Case

“My main use case for StrongDM is to provide access to database credentials. I wanted to give users access to the database and also to the applications that I have built for testing. Providing privileged access to users through StrongDM is the core use case I implemented..”

Verified user[Read full review](#) 

Associate Software Engineer at a computer software company with 201-500 employees

“I have been using StrongDM for around one year as a client. My main use case for StrongDM is to authenticate my user to get access to the cloud environment.

A specific example of how I use StrongDM to access my cloud environment is that I typically need to access Kubernetes resources, and to do that, I use StrongDM to find the resource inside SDM and connect to it. This is the only use case I have..”

Dmitryg Ginsburg[Read full review](#) 

Principal Software Engineer at a tech vendor with 1,001-5,000 employees

“My main use case for StrongDM is Just-In-Time access for connecting to Windows or Linux machines through RDP or SSH.

A specific example of how I use StrongDM for Just-In-Time access is that we have implemented StrongDM as a PAM tool which enhanced the Just-In-Time access for a customer. We did a one-to-one resource mapping with respect to the target systems in each data center. Once we added the resource into StrongDM, with the help of dynamic rules, we can provide access to the relevant users or groups. The users can access StrongDM using the Just-In-Time access and establish a connection via the StrongDM client..”

Verified user

[Read full review](#) 

Senior Solution Advisor at a tech vendor with 10,001+ employees

“My main use case for StrongDM is to assess identity and authentication and authorization access control reviews. When I conduct internal audits or assessments to check the presence of security controls, I use StrongDM to navigate to the configuration settings panel to check what flags and features are enabled or disabled. I appreciate the UI of the overall tool and its functionality.

“There was a situation where I had to check whether the privileged account credentials maintained in StrongDM PAM tool are actually encrypted. I configured and opened StrongDM and checked the settings in the configuration window where I was able to verify that StrongDM contains controls and features which enable it to encrypt privileged account credentials. Additionally, it has features for auditing, generating audit trails, and log trails for all activities conducted by any user who is using privileged accounts. Apart from that, there is a database active monitoring tool embedded within StrongDM. These are certain cases where I have navigated this tool and found the UI to be very user-friendly..”

Verified user

[Read full review](#) 

Solution Delivery Advisor at a tech vendor with 10,001+ employees

“My main use case for StrongDM is privileged access management and infrastructure access that we cater to, as we were looking for alternatives and solutions to securely control and monitor our access to servers. We have been using different kinds of Kubernetes clusters, databases, cloud infrastructure, and internal applications. Instead of giving direct access to our employees, the idea was a VPN-heavy access with shared keys for better usage. This is how I used it during my Kafka experience about three years ago, and also in my current team at GitLab.

“In one of those scenarios, my experience with StrongDM while working with Kubernetes in the Kafka team illustrates how we were initially looking for a better way to manage secure access to our infrastructure. Our teams scaled across different environments and regions, primarily Europe, including Sweden and India. Before using StrongDM, we relied on VPN access and manual permission handling, which became difficult to audit and maintain over time as our team grew. Our main use case was centralized privileged access management for Kubernetes clusters. We also considered using it for Linux servers on-premises for the same application but opted out at that time due to limited usage and some internal platforms running on AWS. We aimed for developers and operations teams to get the access they needed without exposing long-lived credentials.

“StrongDM is instrumental in unifying access across different systems in our organization, alleviating the complications from separate tools. In the Kafka team, we had AWS infrastructure with Kubernetes clusters managing EC2 machines and internal services for different customers referring to our Kafka topics. StrongDM facilitated a centralized approach to access control, audit logging, and temporary authorization. For example, while working on the Kafka platform on EKS, developers and operations teams could utilize a unified access process across various environments, thus streamlining their work..”

Mohit X

Dev Ops Engineer And Solution Architect at Scania

[Read full review](#) 

StrongDM eliminates our weekend outages by providing reliable infrastructure access and improving our user experience. Our engineers can use their preferred SQL clients like MySQL Workbench and MS-SQL. The platform simplifies our compliance by providing detailed session logs and query capture to SOC 2 and ISO 27001 audits, enabling seamless migration and allowing engineers to connect directly to internal resources without exposing the entire network or using cumbersome VPN.

StrongDM offers just-in-time access by automatically granting users temporary or time-bound access to privileged systems and revoking it when the task is complete, enforcing the principle of least privilege. StrongDM replaces our legacy PAM solution with a modern, lightweight platform that simplifies access management, enhances the user experience, and ensures robust security. It enables role-based access control, automates our workflows, eliminates the need for old license rotations, captures every query and keystroke, and ensures compliance following standard frameworks like SOC 2 and ISO 27001. Furthermore, it features an agentless architecture that supports users' preferred tools, reduces friction, and boosts productivity. It also enables centralized multi-cloud access, accelerates growth, eliminates VPN pain with zero-trust security, and secures and streamlines our database access.

“StrongDM provides just-in-time access by automatically granting users temporary or time-bound access; for example, if someone wants to use it for four hours or eight hours, it will specify that to the privileged system and revoke access when the task is complete. Another great feature is total session visibility, as StrongDM acts as a protocol-aware proxy that captures every query, keystroke, and server interaction, creating a comprehensive audit trail required for standard frameworks like SOC 2 and HIPAA. StrongDM eliminates credential sprawl by separating end-user authentication, typically via SSO, from the database's native credentials, so users never need to know or manage raw passwords.

“By adopting StrongDM, we have achieved benefits such as eliminating our weekend outages, streamlining ongoing on-call workflows, enabling seamless migration with POC transitions directly into production with minimal effort, allowing our engineers to use their preferred SQL clients like MySQL, PostgreSQL, and Workbench, and facilitating compliance through detailed session logs and

query capture for SOC 2 and ISO audits.

“StrongDM connects a user to a database or server, but once the session is established, it treats the runtime as a black box and cannot natively enforce fine-grained or attribute-based access control, such as restricting raw column visibility. For a generic TCP resource, StrongDM only records metadata — who, when, and what — instead of capturing the actual commands or payloads executed within the session. .”

AmitRathod

Senior Analyst at Toll Holdings Limited

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“The initial setup was fairly straightforward as we run everything in Docker. From that side, there wasn't much effort required from StrongDM. However, integrating it into our environment was completely on us..”

Patrick

[Read full review](#) 

Senior Devops Engineer at a transportation company with 51-200 employees

The initial setup was on Google Cloud Platform. The deployment was straightforward and easy. As with any deployment, you do have some minor quirks here and there, but compared to whatever we had before, that was an absolute breeze. Mean time to deployment is negligible.

Vlad Gust

[Read full review](#) 

Director at LivePerson

“Concerning pricing, setup cost, and licensing, our experience was very smooth as we chose not to go through the AWS Marketplace but arranged meetings directly with StrongDM. Their team was prompt, and I can say that the pricing and licensing appeared reasonable for complex cloud management. We needed a good product and solid sales service post-purchase, which they provided efficiently and adequately. We compared their offerings with other tools in the market, agreeing on an annual license basis. The setup cost was free, with technical staff aiding our onboarding, requiring us only to cover the license fee..”

Mohit X

Dev Ops Engineer And Solution Architect at Scania

[Read full review](#) 

Customer Service and Support

Customer support is very good; whenever there is a query or issue, they provide support as needed. They also have very good documentation, where they often ask us to refer to a particular document but can provide excellent on-call support.

AmitRathod

Senior Analyst at Toll Holdings Limited

[Read full review](#) 

“I rate technical support seven out of ten because their response takes much more time than usual. However, at the end, they can help. I think they want to reduce their support staff..”

Ibrahim Hassan Barakat

Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

[Read full review](#) 

“The technical support is responsive and knowledgeable. We have a ticketing system and didn't need much direct contact with sales engineers because the support handled our needs well..”

Verified user

Senior Data Engineer at a non-profit with 1,001-5,000 employees

[Read full review](#) 

“That's how we got some of those feature requests in. We've only contacted support one or two times without a feature request. The support interactions have been minimal because of how good the documentation is..”

Patrick

[Read full review](#) 

Senior Devops Engineer at a transportation company with 51-200 employees

“I would rate customer support at StrongDM nine out of ten because we experienced exceptional support during both pre-sales and post-sales. They responded quickly to issues and were readily available for calls rather than waiting for email confirmations. I rate customer support a solid nine out of ten..”

Mohit X

[Read full review](#) 

Dev Ops Engineer And Solution Architect at Scania

Other Advice

“I can share that in terms of the number of hours, as an auditor, if I require 30 hours to audit a PAM tool, with the help of StrongDM, when I am auditing the tool, it will help me to audit the whole thing within 10 hours or maybe 15 hours. This amounts to approximately 50% of the time saved for me as an auditor.

“My advice for others looking into using StrongDM includes its user flexibility, good scalability, and providing advanced features. If they are looking for these things, they should proceed with StrongDM. My overall rating for this product is 9 out of 10..”

Verified user

Solution Delivery Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

“I would assess StrongDM's effectiveness in closing breach paths in real-time as easy and effective, although I have not encountered this type of situation in my test case.

“Continuous authorization is more valuable than periodic checks from my perspective because if something goes wrong during the period of a periodic check, it could be a loss for the organization. Continuous authorization is better.

“My advice for others looking into using StrongDM is to plan everything before integrating it into their organization. It is not suitable for very small startups with fewer resources. It is more useful for organizations that have adopted Kubernetes, VPN access, databases, and manual applications for granting access. These resources can better benefit from StrongDM based on my experience.

“I have rated this review with a score of seven..”

Verified user

Associate Software Engineer at a computer software company with 201-500 employees

[Read full review](#) 

StrongDM uses AI in primary ways, including building and testing its security software with autonomous agents and controlling system access through AI agents. StrongDM has pioneered a unique software development pipeline in its software factory, where AI agents write, test, and deploy production software without human intervention. StrongDM also utilizes a digital twin universe, building virtual behavioral clones of third-party servers such as Okta, [Jira](#), and Slack, allowing it to simulate thousands of customer edge cases and test system failure without risking the production environment. Regarding the guardians of agenticity, it involves AI as a client, and there are AI access policies, ensuring the system watches what AI agents do in real time, instantly blocking or allowing their attempts to read files, connect to services, or make network calls based on human-readable policies.

The accuracy of StrongDM's output is good, and for reliability, it allows attempts to read files, connect to services, or make network calls based on human-readable policies, which makes the reliability very good.

“I have provided a review rating of eight out of ten for StrongDM. .”

AmitRathod

Senior Analyst at Toll Holdings Limited

[Read full review](#) 

“Continuous authorization is significantly more important for us; periodic checks alone might not suffice. In AWS and Kubernetes environments, access needs fluctuate rapidly due to various incidents or operational tasks. Periodic checks only offer visibility at specific points in time, while continuous authorization ensures we retain real-time control, diminish unnecessary standing access, and improve overall security posture.

“StrongDM's credential-less access control was a primary reason for our choice, as managing credentials for various employees and moving consultants was increasingly challenging. The credential-less approach reduces the need to

distribute or manage long-lived credentials, enhancing security and operational simplicity. Its integration with existing secrets managers in AWS was particularly beneficial, aligning securely with our centralized authentication and governance processes, matching our zero-trust practices.

“My advice for others considering StrongDM is that it greatly depends on individual use cases; however, for enterprise organizations seeking end-to-end identity solutions, this is an excellent tool. Many options in the market may lack certain features that StrongDM provides as a comprehensive package. StrongDM excels in compliance management and identity management, so I recommend considering them. I would rate this review as an eight point five overall..”

Mohit X

Dev Ops Engineer And Solution Architect at Scania

[Read full review](#) 

“I am not aware of StrongDM's AI capabilities, including its governance and security.

I don't know about StrongDM's AI capabilities regarding its accuracy and reliability of output since I don't use this feature.

I would say that StrongDM is deployed on-premises in my organization, but I am not certain because I am not involved in those details.

I assess StrongDM's effectiveness in closing breach paths in real time as a very effective way.

I don't have an opinion on the importance of StrongDM's continuous authorization versus periodic checks for my organization.

I am not aware of how StrongDM's credential-less access control integrates with existing vaults and secret managers, but I am getting access to cloud resources and

have not explored those features.

I assess StrongDM's ability to unify access across different systems in my organization as effective; we mostly use access to our cloud resources and work with different cloud providers.

I am not involved in the pricing, setup cost, or licensing, as it is managed by different DevOps teams.

I have not interacted with StrongDM's customer support, so I cannot comment on it.

It is difficult for me to give any advice because I am using StrongDM as a regular user, but I am very satisfied. I give StrongDM an overall rating of ten out of ten..”

Dmitryg Ginsburg

Principal Software Engineer at a tech vendor with 1,001-5,000 employees

[Read full review](#) 

“StrongDM integrates with Dell [Secret Server](#), and we can also integrate it with other PAM solutions. It fetches credentials from the other vaulting tool and establishes connections. It also manages non-human accounts and can establish connections through direct or proxied connections. Credential rotation is handled by the other vaulting tool, so StrongDM acts as a proxy tool over it.

Removing long-standing access has significantly impacted my security posture by ensuring that no user has high privilege accounts or long-standing access without necessity. Access is only provided for a certain stipulated period when needed, which helps prevent hacking.

Since using StrongDM, I estimate around a 60% reduction in effort compared to other PAM tools. The integration allows for user-friendly mapping, even in

disaster recovery scenarios, making it straightforward to configure and highly useful for those needing strong disaster recovery solutions.

StrongDM's approach to credential-less access control aligns with zero trust principles based on Just-In-Time access, ensuring no long-standing privilege exists without necessity, reducing the risk of credential leaks.

StrongDM's AI capabilities increase security posture effectively.

The accuracy and reliability of StrongDM's output are very good. I can fully rely on the output without needing to validate it.

We use [AWS](#) for our private cloud.

We assess the effectiveness of StrongDM in closing breach paths in real time through proof of concept and analyzing the use case with respect to requirement and capability mapping.

I would rate this solution an 8 out of 10..”

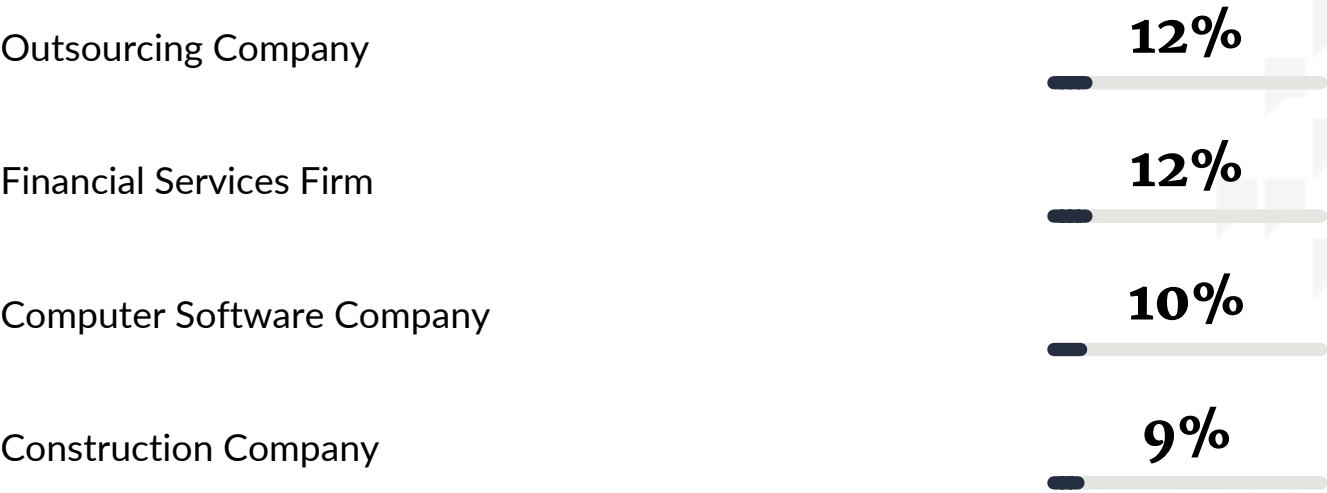
Verified user

Senior Solution Advisor at a tech vendor with 10,001+ employees

[Read full review](#) 

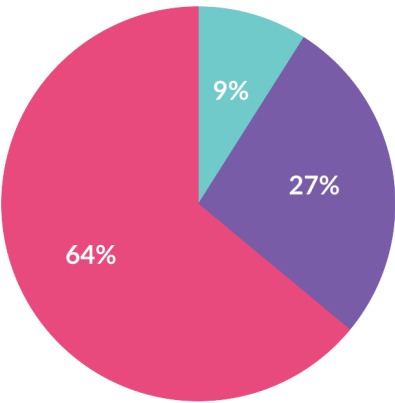
Top Industries

by visitors reading reviews

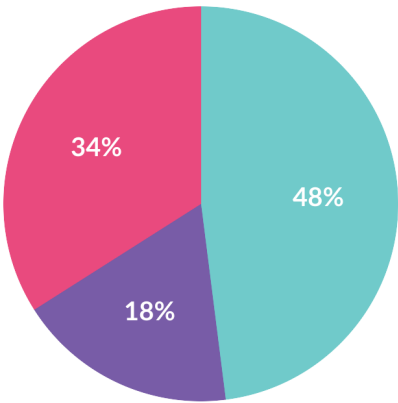


Company Size

by reviewers



by visitors reading reviews



 Large Enterprise  Midsize Enterprise  Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944