StrongDM Architecture Overview

strongdm

Table of Contents

01

Introduction

Over the past decade, identity-based access management has become a standard practice in most enterprises, fortifying their security and compliance efforts. Solutions from identity providers such as Okta, Microsoft Entra, and Google SSO have been instrumental in providing employees with a centralized platform for accessing applications, enhancing both convenience and security measures. However, despite a wide range of tools and technologies, managing access to essential resources is getting more complex.

Legacy solutions do not provide the necessary capabilities to securely and effectively address the modern requirements for privileged access management, and demand far too much manual intervention to operate. They are built to address access as a one-off event, but do not provide the necessary insights for administrators and security teams to investigate and address user behavior post-access. This leaves major security and compliance gaps that actually create additional layers of vulnerability for enterprises.

This challenge becomes even more pronounced as organizations embrace hybrid cloud and multi-cloud environments, introducing additional layers of complexity. How can enterprises streamline access to technical infrastructure when confronted with a myriad of access workflows, protocols, and processes spanning AWS, GCP, and on-premises relational databases?

Addressing this dilemma necessitates innovative solutions that prioritize enterprise security and compliance while offering unified access management across disparate infrastructure components. Such solutions should not only streamline access workflows but also ensure adherence to regulatory requirements and industry best practices, safeguarding sensitive data and mitigating security risks effectively.

Over the last decade, identity-based access management has become commonplace in most organizations. Tools like Okta and Google SSO actively enable employees of organizations to have a single location to find and access their applications. However, access to infrastructure continues to lag behind.

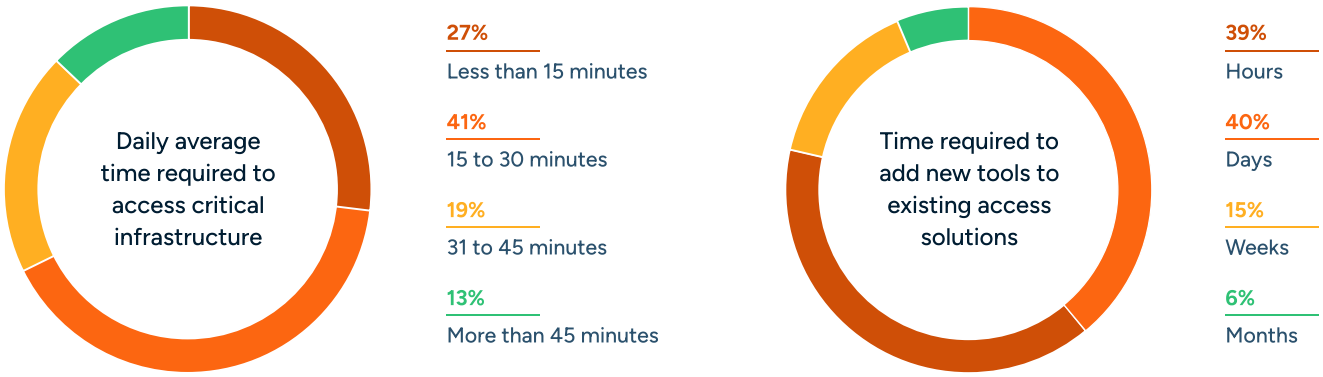
To date, there has been no single tool that connects to virtually every technology in the modern stack. Whether dealing with legacy systems like mainframes or modern solutions like Kubernetes, enterprises face the daunting task of ensuring secure and compliant access across their entire infrastructure landscape. This problem compounds as organizations embrace hybrid- and multi-cloud environments. How do you simplify access to technical infrastructure when the variety of access workflows, protocols, and processes vary widely from AWS, to GCP, to relational databases hosted in your data center?

Privileged Access: Puzzle Pieces That Don't Fit

The modern stack is virtually limitless. It can incorporate everything from databases, to cloud service providers, to servers, to containers—you name it. While each of these systems was designed to solve a particular problem, secure and easy access across systems isn't one of them.

The outcome is tangible—our latest research shows that **73%** of technical staff spend 15 or more minutes simply getting access to the tools they need to do their jobs. And when trying to add new tools, nearly **60%** of respondents state it takes days, weeks, or months for those tools to be added to their existing access solutions. These challenges directly impact DevOps and engineering teams by limiting their ability to successfully do their jobs.

This is the challenge that StrongDM addresses by delivering dynamic access: Credentials and access only exist in the moments they are needed.



02

Product Guiding Principles

The StrongDM platform was built to meet the unique needs of modern enterprises by providing a blend of security, simplicity, and compliance. It operates via continuous verification and validation of identity, right-to-access, and auditability. Once a user is authenticated, the tools and policies of Zero Trust PAM ensure that their authorizations are continuously monitored in real-time, dynamically driving change or dynamically enforcing security access controls.

With StrongDM, enterprises can ensure that only the right people have the right access to critical systems, significantly reducing the risk of data breaches. Our platform supports a wide range of protocols and systems, making it versatile for various enterprise needs. StrongDM's commitment to a **Zero Trust security model** aligns with modern cybersecurity frameworks, ensuring that every access request is authenticated, authorized, and encrypted. By streamlining access management, StrongDM security and compliance teams maintain high-security standards, comply with regulatory requirements, and improve operational efficiency.

It was built on these precepts:

Trust must be assessed continuously

Zero Trust means that determining whether a user (person or machine) should have access to a system or data needs to be assessed throughout every session, not only when they attempt access. With context-based assessment, access needs to be severed immediately if trust is no longer achieved.

Trust must be applied universally

Access management does not work if it only supports part of the stack, leaving other parts vulnerable. Further, tech stacks are not static – they evolve constantly. The dynamic nature of infrastructure is compounded by the use of ephemeral technologies like Kubernetes. Access management must support all critical infrastructure, from legacy systems to modern cloud-native infrastructure and ephemeral resources. Secure access controls must apply to developer environments, proof-of-concept systems, and other technical resources that may not be mission-critical but, if breached, could create a path to critical systems.

No one should have access unless it's actually being used

Shared credentials and standing access grants add to an organization's risk profile because they are vulnerable to malicious actors who could use those grants to gain access. Organizations should mature their access policies/procedures away from simple identity-based access and toward Zero Standing Privilege, using Just-in-Time access workflows to reduce risk caused by perpetual, standing grants.

Credentials that can be seen are assumed to be breached

If a password or credential for a critical system can be seen, there is a high likelihood that it has been shared or documented in code. Every effort must be made to prevent users from ever seeing credentials.

Complete visibility is an absolute necessity

You'll never come to the correct conclusion during an investigation or audit if you don't have all the information. Modern security requires comprehensive audit logs (and session recordings where applicable) of all the actions taken by everyone in your staff – admins, developers, data analysts, and contractors – across your entire stack.

People will find a way to avoid security if the process is too complex

"Secure Access" and "Easy to Use" must not be at odds. To ensure full adoption and compliance, the end-user experience must be simple and eliminate all complexity from the process of accessing resources, from making a request to actually connecting to the resource. Security tools must be designed to make developers' jobs easier. Otherwise, technical staff will find workarounds that undermine security. Core design principles must support developers' native tooling, automation, and workflow or risk undermining the intended result.

These guiding principles drive outcomes that not only improve usability and overall security but also increase the adoption of StrongDM products over time. The intent is to enhance security while reducing friction and complexity for end users, resulting in products that strengthen an organization's overall security posture while also improving end user and admin productivity in a simple and streamlined way.

03

Architecture Overview & Key Concepts

Product 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:

- **Security & Compliance**: Security and compliance teams can gain full visibility into "who did what when" on each system, including video playback of what 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.
- **DevOps**: DevOps teams can provision and deprovision access to specific instances, servers, or databases, in a matter of clicks.
- **Admins**: Access to critical infrastructure can be granted and revoked quickly and easily, greatly simplifying user onboarding and offboarding, provisioning for third parties, and the ability to provide access for a specified period of time. Users, roles, and access are easily managed via an Admin UI (CLI available as well).

StrongDM consists of a few core concepts required to provide access to virtually any tool or system in your infrastructure. These include the StrongDM Control Plane, Gateways, Relays, and the StrongDM Local Client. When an access request is made, these components play a key role in determining if access should be granted, provisioning the credentials, and ensuring that the correct level of access is provided.

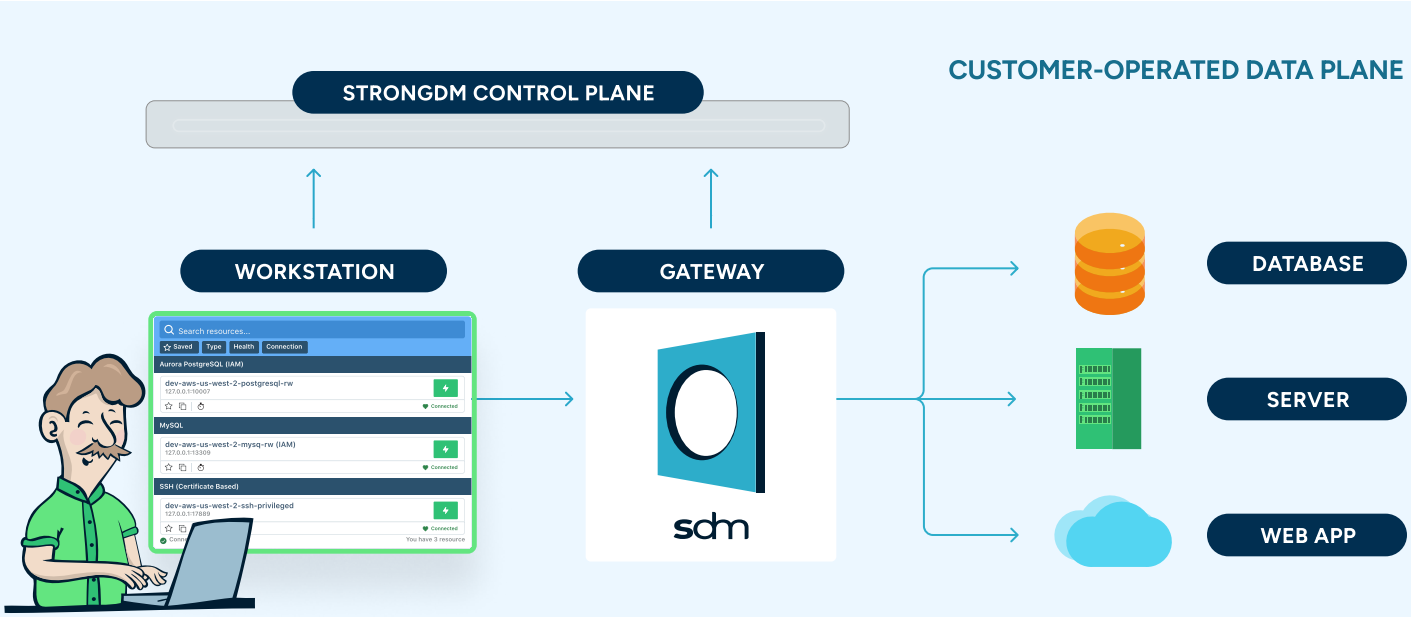
A key strength of the StrongDM network architecture is its use of both forward and reverse proxies, meaning you don't need to change your existing firewall and network Access Control Lists (ACL).

Here is an example:

- Anne authenticates with her identity provider on the StrongDM Desktop App. If required, she will be prompted to provide additional authentication factors, such as MFA or token-based authentication.
- Anne uses the StrongDM Desktop App on her workstation to try to connect to a MySQL database.
- Anne's request is sent to the StrongDM Control Plane, which determines whether Anne's role should have access to that database, and what level of access should be granted (admin, read-only, etc.).
- Anne's request is sent to SentinalOne or Crowdstrike to make sure that the device from which she is requesting is healthy.
- Anne's request is also simultaneously sent to the StrongDM Gateway, which will connect her to the database, provided that the StrongDM Control Plane approves Anne's request.
- If approved, Anne is connected to the appropriate database.

During this process, it's important to note that Anne and her workstation never have access to—or see—the credentials required for access to the database. By **eliminating passwords from the end user**, an organization's risk of threats such as phishing is reduced. Furthermore, customers own the entire path between users, workstations, and infrastructure.

We call this the **Customer-Operated Data Plane**.



Customer-Operated Data Plane

The Customer-Operated Data Plane is the horizontal path between the user, the gateway, and the network segment to the resources being accessed. This has important security and compliance implications, as any sensitive data being accessed is accessed entirely within the customer's infrastructure. For example, compliance requirements ranging from GDPR to SOX to HIPAA all have strict rules regarding how data is managed within an organization.

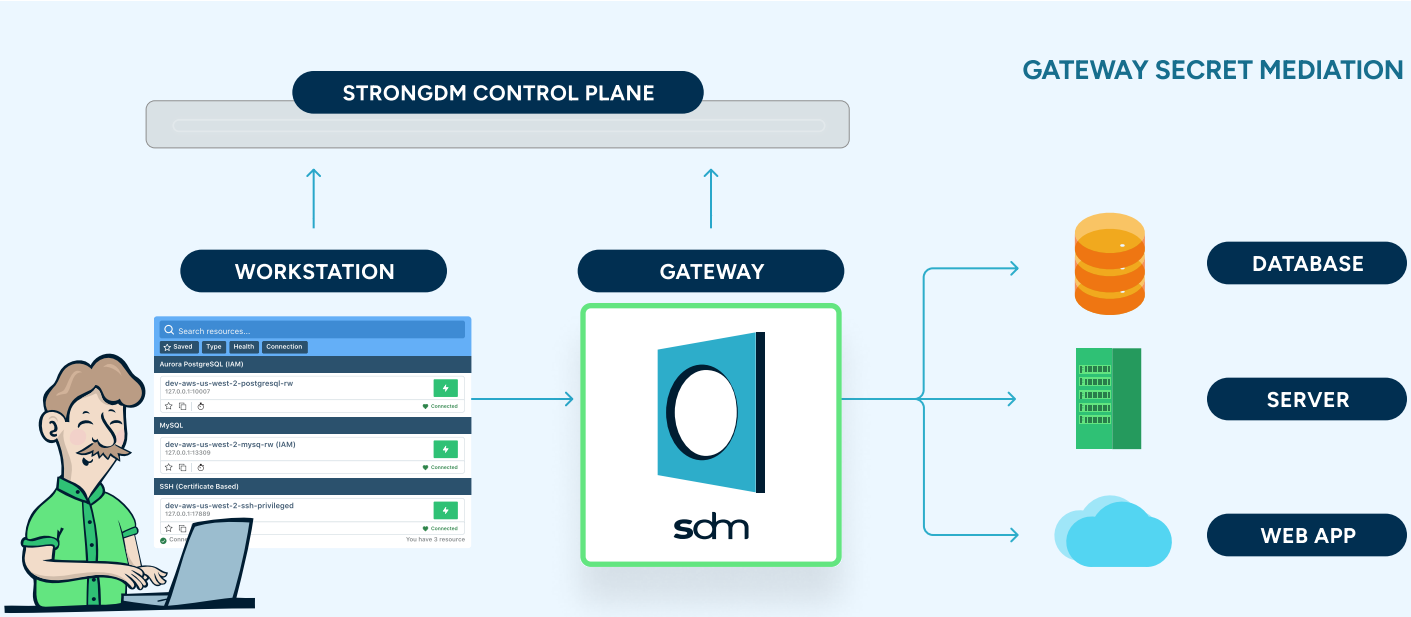
StrongDM Control Plane

The StrongDM Control Plane consists of the Admin UI and access management controls. This is where admins provision and deprovision access, create or change roles, and manage StrongDM system configurations. Furthermore, all Gateways and Relays in the StrongDM network download their configurations from the StrongDM Control Plane.

StrongDM Desktop App

Represented by the "Workstation" above, the StrongDM Desktop App exists on each end user's workstation. The StrongDM Desktop App enables end users to gain access to infrastructure based on their role as defined in the StrongDM Control Plane–this is often known as role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (PBAC). End users can use either the StrongDM Desktop app or the command line to request access to systems. The desktop app then tunnels requests from the workstation to a gateway.

The desktop app is available for macOS and Windows. CLI clients are available for macOS, Windows, and Linux, and users can authenticate to the Desktop App via a login or optimally through an identity provider or SSO.



Gateways

Gateways are the entry point to your network. Requests from the StrongDM Desktop App are sent to a Gateway, where the request is decrypted, logged, and conveyed to the database or server using a StrongDM native protocol for that system. Gateways can be deployed with a DNS entry and/or sit privately on the corporate network behind a VPN. Gateways are deployed in pairs and scale horizontally.

Gateway Secret Mediation

When an access request is made, all secrets remain and are kept between the Gateway and backend systems. Credentials are never shared with the workstation or end user. That means end users **never** have access to credentials, helping to minimize the risk associated with stolen or lost credentials.

Relays

Relays are used in environments that require an egress-only network, such as those that must meet stringent compliance requirements or adhere to security frameworks such as ISO 27001. In these situations, Relays, much like Gateways, are how the StrongDM network connects with end resources such as databases and servers.

Unlike Gateways, Relays do not listen for client connections. They're put in place as the last hop to connect directly to the target. When used, a Relay initiates an outbound connection to the Gateway, creating a reverse tunnel into secured networks where inbound traffic is not allowed.

StrongDM is designed to scale with your organization's needs, particularly in terms of deploying Gateways and Relays to manage privilege access effectively across your environment. Here's how it typically scales:

- **Elastic Infrastructure**: StrongDM leverages cloud-native technologies to allow for elastic scaling. This means that as your organization grows and your infrastructure needs change, StrongDM can dynamically allocate resources to accommodate these changes. Whether you need to deploy additional gateways or relays to handle increased traffic or expanding infrastructure, StrongDM can scale up or down accordingly.
- **High Availability**: StrongDM enables high availability by distributing gateways and relays across multiple geographic regions or availability zones. This redundancy minimizes the risk of downtime due to hardware failures or network issues and ensures continuous access management even in the face of disruptions.

- **Load Balancing**: To optimize performance and resource utilization, StrongDM employs load balancing techniques. Incoming traffic is distributed evenly across available gateways and relays, preventing any single component from becoming a bottleneck. This load balancing mechanism allows for efficient utilization of resources and ensures a consistent user experience even during peak usage periods.
- **Auto-scaling**: StrongDM can be configured to automatically scale resources based on predefined criteria such as CPU utilization, memory usage, or incoming traffic. With auto-scaling enabled, the platform can dynamically provision or deprovision gateways and relays in response to changing workload demands, ensuring optimal performance and cost-efficiency.
- **Centralized Management**: Despite the distributed nature of its infrastructure, StrongDM provides centralized management and monitoring capabilities. Administrators can easily provision, configure, and monitor gateways and relays from a unified console, simplifying operational tasks and ensuring consistent policy enforcement across the entire environment.

Overall, StrongDM's scalability features enable organizations to seamlessly adapt to changing requirements, whether it involves accommodating growth, ensuring high availability, or optimizing resource utilization. By leveraging cloud-native technologies and advanced management capabilities, StrongDM provides a robust and flexible solution for privilege access management at scale.

Agentless Architecture

StrongDM **does not require agents** to be installed on individual systems in order to make a connection. As long as there is a connection between a Gateway and an end device or Gateway and associated Relay, a connection to the system can be made. Because agents are not used, deployment and updates can be executed in a simple and efficient manner.

Platform Security

StrongDM is a distributed system of clients and proxies, coordinated by a central API. Platform security is achieved through three main components:

- Separation of duties among the component systems
- Mutually verified cryptographic identities among each of the system participants
- Immutable activity log collection and reporting

Data Lake

Data lakes have become increasingly popular resources for storing and processing massive amounts of diverse data. Implementing access control policies explicitly tailored for data lakes has now become an essential part of any agile infrastructure, especially because data lakes are expected to deliver necessary data as needed by a growing set of users who need it for daily tasks.

StrongDM enables administrators to define granular access controls based on user roles, attributes, and contextual factors. This ensures that only authorized individuals can access and manipulate data within the data lake, reducing the risk of unauthorized access and data breaches.

The **fine-grained access control** approach offered by StrongDM allows organizations to define granular access controls for their data lakes based on user roles, attributes, and contextual factors. Administrators can easily manage access permissions for individual users or groups, ensuring that only authorized individuals can access specific data sets or functionalities within the data lake.

By addressing these key aspects of data lake security, organizations can effectively protect their sensitive data, mitigate the risk of data breaches, and ensure compliance with regulatory requirements and internal policies.

Analytics & Insights

You can't solve what you can't see. Security and compliance teams need insights into activity within their environments and context to know how they can resolve issues.

StrongDM uses a comprehensive Reports Library, to give leaders visibility into how access is being used, help them enforce **least privilege access**, and understand their PAM deployment. Together, these technologies enable organizations to have total visibility over their access grants.

These insights enable security teams to achieve true Zero Trust access by providing these **dashboards**:

- **Standing Access** dashboard to view what permissions have not been used over a specific time period. Use insights to revoke any unused access privileges and the implement workflows for Just-in-Time access.
- **Auditor Insights** dashboard allows security teams to know exactly who has access to what, through which role, at any given time. Complete audits more efficiently with out-of-the-box reports for access policy questions.
- **User Activity** dashboard shows the number of sessions that have occurred and for how long. It enables teams to create alerts for unusual behavior and to better understand access behavior patterns around your most sensitive resources.
- **Executive Summary** dashboard is a comprehensive view of standing access across your organization. It provides insights into permissions that have remained inactive over a specific time frame, empowering decision-makers to identify and revoke any unused access privileges efficiently. The Executive Dashboard shows Just-in-Time access workflows, which enables administrators to implement timely adjustments to access permissions, ensuring optimal security posture without unnecessary access clutter.

Centralized Policy Management

Writing policies once and enforcing them everywhere is the dream. StrongDM simplifies policy management by extending your existing RBAC and ABAC policies with new signals and controls. This centralized approach streamlines administration, reducing the complexity of access control. With StrongDM, you can establish security measures that are uniformly enforced across all your diverse applications and infrastructure components. It builds upon the natural strengths of these resources by adding layers of security policies, thereby improving the existing controls and safeguards.

The powerful Strong Policy Engine, driven by the **Cedar Policy Language**, facilitates the decentralized implementation of centralized policies, establishing a secure and cohesive access control framework throughout your infrastructure. This engine enables policy evaluation with response times in the sub-millisecond range, in line with the high-performance standards that users of StrongDM have grown accustomed to. Policies are managed and enforced through these components within the Strong Policy Engine:

- **PDP (Policy Decision Point)**: This is an engine that evaluates policies against the current context (e.g., user role, resource being accessed, environmental conditions) to make a decision (allow, deny, challenge, etc.). The PDP informs the PEP (see below) of its decision, which the PEP then enforces.
- **PEP (Policy Enforcement Point)**: This function intercepts users' actions at the application level or data level to make policy decisions or enforce policy decisions made by a PDP. The PEP acts as the gatekeeper, ensuring that only legitimate requests, as defined by the policies, are allowed to proceed.

- **PAP (Policy Administration Point)**: A tool or interface used by administrators to manage policy rules. The PAP enables the creation, deletion, and modification of policies, which are then stored in the Policy Retrieval Point (PRP) and enforced via the PEP/PDP mechanism.
- **Policy Information Point (PIP)**: The Policy Information Point (PIP) supplies the Policy Decision Point (PDP) with up-to-date data essential for informed access decisions. This includes user attributes (such as roles or department), resource details (like classification levels), and contextual factors (such as time of day or geographical location). It is the PIP's duty to collect this information from diverse sources, including databases, directories, or external systems, and furnish it to the PDP upon request. The PDP's capacity to render precise decisions hinges on the quality and promptness of the data supplied by the PIP.

Workflows

StrongDM **Access Workflows** ensures that your team can get access to the tools they need when they need it and also makes it possible to remove that access just as quickly. This approach eliminates standing credentials by streamlining access requests that meet security policies. StrongDM Access Workflows delivers:

- **Enhanced Security**: Access is only granted for a specified duration eliminating the need for standing access and reducing the overall attack surface.
- **Improved Efficiency**: Easier to manage user rights with JIT access; no need to keep track of who has standing permissions.
- **Reduced Insider Threats**: No more persistent access to sensitive data. With JIT access, the potential damage an insider can cause is confined to a narrow access window.

StrongDM Access Workflows significantly improve the end-user experience. End-users have an individualized Access Catalog to resources available based on their role or resource attributes (i.e., environment tags, geo-location, etc.). Users request access and connect based on human or automated approval.

Open APIs

The StrongDM API allows users of StrongDM to programmatically interact with their organization in StrongDM in order to create, remove, or manage users, roles, permissions, gateways, relays, resources, and more. The amount of API access afforded to an API key depends entirely on what was granted to the key by the organization's administrators when the key was created.

The **StrongDM API** is constructed with **gRPC** and a request signature model that requires the use of one of the StrongDM SDKs to interface with the API. The SDKs were designed with REST principles in mind. They are built around a set of domain objects, as well as the basic set of Create, Read, Update, and Delete (CRUD) operations.

Moreover, the **StrongDM Audit API** provides advanced auditing and logging capabilities that simplify how data is extracted from StrongDM for programmatic integration into other parts of your organization, such as SIEM, log aggregators, compliance and/or security reports, or end-to-end IAM workflows. You can also use the StrongDM API to do the following:

- See the history of what happened in your organization.
- View full snapshots.
- Look at shells for all replays.
- View SSH session data as it comes in, and watch sessions play live.
- Actively look at queries as they come in.
- Suspend users by ID.

04

Key Features

Customer Maintains Control

StrongDM embraces a “zero knowledge” methodology. That means customers should maintain control of all their data, passwords, and credentials at all times. This minimizes the chances that passwords or data get compromised, as third parties have the minimal amount of access necessary and should not be able to read your logs.

Native Protocols

StrongDM offers native protocols for a large number of technologies. The use of native protocols for infrastructure access is critical, as virtually every part of your stack may have different login requirements or workflows necessary to provide access. StrongDM was designed to onboard new protocols without the need for professional services. While technologies like databases have been supported since the product’s inception, it is easy to add new frameworks when required. New technologies are constantly being added to the StrongDM list of native protocols. **See the full list**.

Resource Credentials And Cloud-Native Resource Authentication

StrongDM is a protocol-aware proxy that injects **credentials** during the “last mile” hop between the proxy and the target database or server. This feature seamlessly integrates authentication mechanisms within cloud-native environments, enabling secure access to resources and services. By injecting credentials dynamically, the Gateway facilitates streamlined authentication processes, ensuring that only authorized entities gain access to sensitive data and functionalities. Furthermore, this capability enhances scalability and flexibility, allowing organizations to adapt to evolving authentication requirements in dynamic cloud-native infrastructures.

As a result, sensitive credentials are always inaccessible to users and are never transferred to a StrongDM client in any form. Once needed, credentials are unlocked at runtime using a “dual-key” system. In order for credentials to be unlocked, the following must be true: A cryptographically valid proxy instance requests decryption on behalf of a cryptographically valid user session. Neither the user nor the proxy instance alone is sufficient to decrypt a credential.

Authentication can be done in two different ways. With certificate-based authentication, a digital certificate is used to identify and authenticate a user, device, or machine. The other type, cloud native authentication, makes it easy to authenticate to cloud resources using their native methods, taking advantage of their ephemeral properties.

Users can be granted access to a datasource or server via a role or temporary access. From a database or server perspective, this access is conducted via a Leased Credential.

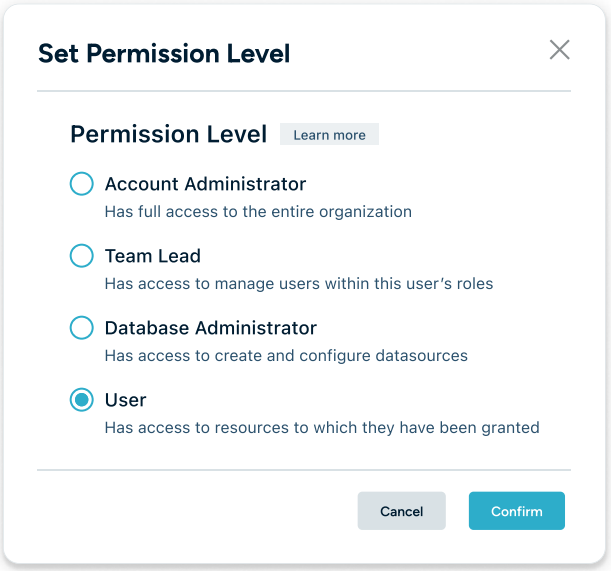
User Authentication

Users can authenticate into StrongDM via delegated authentication, native accounts, or hybrid. StrongDM can integrate with Duo Security to enforce multi-factor authentication (MFA) on all StrongDM client sessions.

Authentication Model	Description
Delegated	The most common mode of authentication into StrongDM. Authentication is delegated to a directory tool (such as Microsoft Active Directory) or single sign-on (SSO) provider (such as Okta or Google).
Hybrid	A hybrid approach can be helpful in situations where multiple teams or contractors need access. Members of the organization are able to authenticate via a directory or SSO, while third parties can use native accounts.
Native Accounts	Native accounts are required for StrongDM administrators and may be used in cases where a directory or SSO is unavailable.

Admin UI

The StrongDM Admin UI is where admins can provision and deprovision access, configure roles, review logs, view replays, add infrastructure, and adjust the network and settings. When end users ("User" below) log in to the StrongDM Admin UI, they can only view links to download the StrongDM Desktop Application and CLI and access product documentation.



Feature	Description
Logs & Replays	View user and access logs as well as SSH, RDP, and Kubernetes replays via the Admin UI.
Access Management	Manage users, roles, accounts, and generate API keys.
Infrastructure Management	Add, change, and remove data sources, servers, clusters, websites, and cloud services.
Network	Manage Gateways, Relays, and secret store integrations.
Settings	Manage integrations with identity providers, authentication settings, ports, SSH, and log encryption and storage.

Policy Management

Effective policy enforcement and management are crucial for organizations to achieve security, compliance, and operational efficiency. Many organizations struggle with cumbersome processes that result from an explosion of roles and reliance on duplicative, disjointed solutions. The StrongDM Policy Engine provides a simple, adaptable, and cohesive approach to policy enforcement and management, and organizations can ensure that their policies are consistently applied across all systems.

With StrongDM, you can control which groups of users have access to which resources, what credentials are being used, and log actions that occur. Policies take this binary "yes or no" access grant much further by allowing you to inject specific conditions into these interactions. With policies, the user's **contextual elements**, such as location or device trust, are evaluated in order to make dynamic access decisions. The audit trail of particular actions can also be enhanced by requiring a user to justify an action taken on a resource.

The **Policy Library** contains a listing and brief description of each policy that has been created in your organization. Clicking the name of any policy, or the Details button, opens the details view for that policy in the Policy Editor tab.

- You can define policies to enforce fine-grained access control over pre-assigned grants.
- To gain access to a resource, a user must be a member of a role that grants that access or have temporary access via an access request.
- The policy statements take this further by conditionally allowing or forbidding that access given certain options.
- Any further policies written add fine-grained access controls to those grants and allow more fine-grained context to be applied.
- This context can include items such as the location of the user, device trust status, and others.
- These signals give the ability to consider more context when allowing resource interactions beyond whether the user has been granted access or not.

Logging

Logging is fully configurable. You can control what passes to StrongDM, and you have the option to log in with StrongDM, log locally, or both. Logs stored with StrongDM are written to an immutable, write-once Amazon S3 bucket. By default, logs stored with StrongDM are retained for a period of 13 months and then are permanently deleted.

For organizations that choose to log locally, logs are written to the StrongDM Gateway's local storage. This allows you to configure how and where to ship logs–for example, sending them to a SIEM or log aggregation tool.

What is Logged?

Every user authentication, query, SSH, and RDP command, as well as administrator actions such as permission changes.

Log Encryption

StrongDM offers three encryption methods for customers to choose from:

- Separation of duties among the component systems
- Mutually verified cryptographic identities among each of the system participants
- Immutable activity log collection and reporting

Log Administration

Administrators have a variety of controls over logging, including configuring resource logs, queries, SSH, RDP replays, and more. This also includes determining whether logs are stored with StrongDM or locally.

Tamper Evident

Every action within the StrongDM application is logged in a repository that is not accessible to account administrators. This ensures that bad actors are unable to access the logs that are keeping a record of activities within each system.

Auditing & Audit History

Admins can review a variety of data points either as they exist or as existed at any point in time in the past.
This history can be exported in a number of formats, including JSON and CSV, to easily provide evidence to auditors or to feed to internal tooling.

Policy Engine

A policy engine allows an organization to manage, enforce, and audit rules across its system. It is designed to provide a centralized point of control for policy management, reducing the complexity of managing rules in large and distributed systems.

Continuous Zero Trust Authorization builds on top of StrongDM's already robust capabilities for delivering dynamic access to infrastructure and tools with a new policy engine, centralized policy management, and the ability to add nearly any context to real-time policy enforcement.

The Strong Policy Engine, powered by the **Cedar Policy Language**, enables distributed enforcement of centralized policies, creating a secure and unified access control framework across your infrastructure. The engine allows for policy evaluation with sub-millisecond response times, aligning with the high-performance standards that StrongDM users have come to expect. It includes the following components:

Centralized Policy Management

StrongDM simplifies policy management by extending your existing RBAC and ABAC policies with new signals and controls. This centralized approach streamlines administration, reducing the complexity of access control. With StrongDM, you can establish security measures that are uniformly enforced across all your diverse applications and infrastructure components. It builds upon the natural strengths of these resources by adding layers of security policies, thereby improving the existing controls and safeguards.

Attribute-Based Authorization Models for Zero Trust

StrongDM supports various authorization models, including *BAC (Anything-Based Access Control), **Role-Based Access Control (RBAC)**, **Attribute-Based Access Control (ABAC)**, and **Policy-Based Access Control (PBAC)**. You have the flexibility to choose the model or blend of models that best suits your needs.

Context-Based Signals for Granular Control

To enhance granular control, StrongDM uses context-based signals like geography, device trust, IP, requestor data, or resource tags to access decisions. This provides additional information about the requester, the resource being accessed, and the environment. Coupled with continuous trust assessment, Context-Based Signals allow organizations to roll out an adaptive security strategy that responds to changes in real time.

Strong Vault

Strong Vault is an encrypted, central repository where secrets, keys, and credentials can be kept. It is implemented using AWS Key Management Service, and leverages authenticated encryption with associated data (AEAD) via the KMS Encryption Context. Strong Vault prevents the exposure, loss, or theft of these credentials. Additionally, all decryption events are written to a tamper-hardened audit log owned by a separate AWS account. It uses the following:

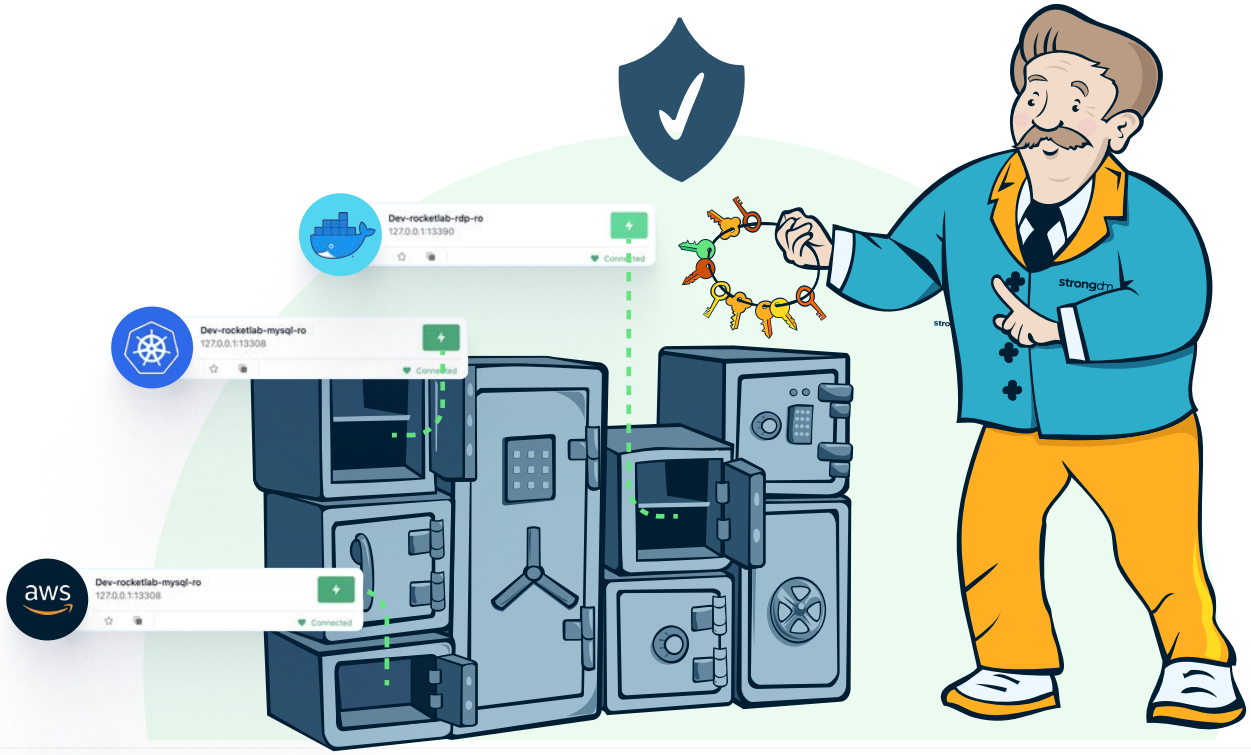
StrongDM Secret Store

StrongDM Secret Stores are implemented using the AWS Key Management Service (KMS). It uses authenticated encryption with associated data (AEAD) via the KMS Encryption Context. All credential events are written to a tamper-hardened audit log that's owned by a separate AWS account.

Third-party Secret Stores

StrongDM also provides the option to integrate with third-party secret stores to store resource credentials. If your organization already manages and rotates credentials via a supported secret store, you can continue to use that workflow with no changes. You can learn more about StrongDM's secret store integrations in our documentation.

It should also be noted that StrongDM is secret vault-agnostic, and **organizations can use their vault of choice**, whether that be Azure Key Vault, CyberArk Conjur, CyberArk Digital Vault, Delinea Secrets Server, Hashicorp Vault, GCP Secrets Manager or Amazon Secrets Manager.



Reports Library

The Reports Library works with the StrongDM Audit API to enable organizations to answer common user queries regarding infrastructure access for audits, investigation, and compliance use cases.

The Reports Library provides admins with a complete view of resources and roles that are over-privileged and underutilized, as well as reports on resource grants to sensitive resources in an easy and automated manner across the entire infrastructure.

Pre-packaged reports include:

- **Auditor Insights**: Shows exactly which resources users have access to based on roles and how they are granted that access at any given time. Answer auditor questions quickly and remain compliant.
- **Standing Access**: Understand the security risk profile of all standing access grants. Make decisions on who should continue to have access and where access can be revoked without introducing friction.
- **Executive Summary**: Provides a high-level overview of security posture as it pertains to privileged access management. Know what percentage of grants and resources are being utilized at any given time.
- **User Activity**: Tracks user activity and behavior within StrongDM. This report highlights any problematic sessions based on concurrency or length of sessions. Take advantage of the user activity report when researching security incidents to know exactly what sessions are being run.
- **Access Workflows**: Understand exactly how Just-in-Time access is utilized and optimized in your organization. Create automated workflows for repetitive access requests, or remove access to resources that aren't being used.

Access Workflows

Access workflows manage the process and logic around the lifecycle of an access grant. This includes providing users with a directory of roles and resources they can request access to, support for multi-step processes and change management, and the ability to use out-of-the-box integrations with ticketing and ChatOps tools, such as ServiceNow and Slack.

Integrations With Industry Standards

StrongDM integrates with a variety of industry standards in order to connect with new and existing solutions. See below for the list of industry standards that StrongDM currently integrates with, as well as links for more information.

1. SCIM
2. OpenID Connect
3. SAML
4. OAuth

05

We 💗 Your Stack

StrongDM's native protocols range from the most common relational databases to new and emerging technologies used by early adopters. Below are some highlighted technologies that StrongDM supports.

Databases	SSO & Identity Providers	Cloud Service Providers	Logging	Containers & Kubernetes	Device Management
Amazon RDS	Auth0	AWS	Datadog	AKS	CrowdStrike
Cassandra	Azure AD	Azure	FileBeat	Docker	SentinelOne
IBM DB2	GSuite SSO	Cisco HCI	Logentries	EKS	And more!
MongoDB	LDAP	Dell EMC	Loggly	Kubernetes	
MS SQL Server	Okta	GCP	LogRhythm	And more!	
MySQL	OneLogin	Heroku	Logstash		
Oracle RDBMS	OpenID	Rackspace	Amazon S3		
Postgres	Connect	And more!	Splunk		
Redis	SAML		Sumo Logic		
Snowflake	And more!		Syslog		
Sybase			And more!		
Teradata					
And more!					

Oh wait–did you notice there's more? For the full list, please visit strongdm.com/connect.

06

Conclusion

Modern stacks have grown to a complexity where it is difficult, if not impossible, to manually manage privileged access across your entire organization. The combination of different technologies, different roles, different levels of permissions, and constantly evolving technology are driving a critical need to streamline how infrastructure access is managed and enabled. These are the core challenges that StrongDM addresses.

To learn more or request a demo, please visit www.strongdm.com/get-a-demo.

strongdm

StrongDM provides a dynamic access platform that gives every business secure, dynamic access controls that people love to use. Trusted by the Fortune 500 to fast-growing businesses like SoFi, Chime, Seismic, and Better, StrongDM gives businesses the control and visibility they need at the speed they want, with one platform that works for every environment. Connect with us on **LinkedIn**, **X**, **Facebook**, **YouTube** or head to **www.strongdm.com** to learn more.