StrongDM™ Dynamic Access Management (DAM) Platform

Secure, dynamic and auditable access to every resource in your infrastructure.

GRANULAR CONTROL

Protect your resources with real-time monitoring and granular access controls that give people just-right access every time.

FOR ALL ACCESS AND ACTIONS

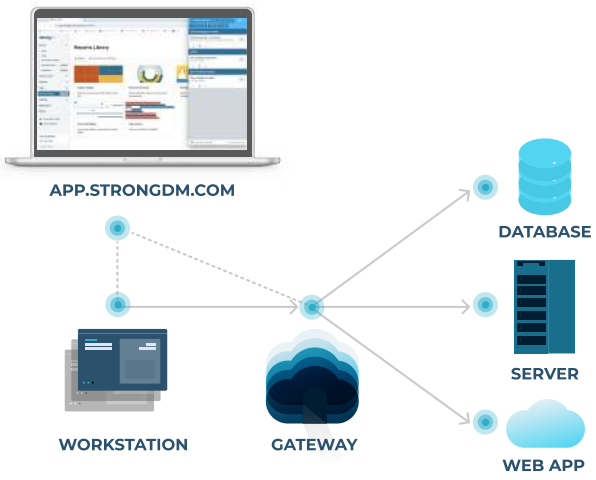
Complete visibility across your entire infrastructure for every connection. Access is assessed and granted based on contextual factors.

WITH STRONG POLICY ENFORCEMENT

Distributed policies can be enforced anywhere on your network, regardless of the system, tool, or location an activity is taking place.

How it works

StrongDM is a proxy that manages and audits access to databases, servers, clusters, and web apps.



The Gateway

Gateways are the entry point to your network. They can be deployed at your edge with a public IP or DNS entry, sit privately on the corporate network, and/or behind your existing VPN solution.

In the case of a flat network, it's the gateway that talks to the target systems. If internal subnets disallow ingress, relays create a reverse tunnel to form connections to the gateway. All data routes through your network.

Gateways decrypt credentials on behalf of end users and deconstruct requests for audit purposes. Gateways and relays are deployed in pairs and scale horizontally.

Local Client

The local client tunnels requests from the user's workstation to the gateway, through a single TLS 1.2-secured TCP connection. strongDM supports Mac, Windows, and Linux workstations.

To authenticate, users login to the local client or can be optionally redirected to your identity provider or SSO. The local client consists of both graphical and command-line interfaces.

Configuration Layer

The Admin UI houses configuration. Users are assigned to roles, and roles are collections of permissions across servers, databases, clusters, and web apps. Configuration is pushed down to the end user's local client and updated in real-time.

Top 10 considerations for a dynamic access platform

Table stakes for supporting a modern stack

- Complete protocol support for SSH, RDP, K8s, & DB workflow
- Configurable credential storage, rotation, and dynamic checkout
- No agents or software deployed to your servers
- Full auditability & replay of all supported protocol sessions
- RBAC, ABAC, PBAC, and JIT access support
- Native SSO integrations, including SCIM
- Centralized policy management with sub-millisecond repose times for policy evaluation and enforcement
- Fully configurable, encrypted log storage
- Eliminate credential exposure to end users
- Robust reporting

Key Capabilities

Authentication

Determine who gets access to your infrastructure

- Integrate with identity providers to centrally manage infrastructure acces
- Automate user & group provisioning with a single source of truth
- Store credentials securely with the Strong Vault or use an existing secrets manager
- Native MFA integration
- Full SCIM 2 provisioning for users and role
- SSO support through SAML
- Full OIDC support for any OpenID /OAuth identity provider
- Context-based signals like geography, device health, IP, or requestor data for authentication decisions

Networking

Connect your staff to whatever they need

- Replace VPNs and bastion hosts with a secure Zero Trust network
- Self-healing mesh network of proxies
- Highly available strongDM API inherits redundancy from AWS
- Mutual TLS network connections

Authorization

Specify what and how much staff can access

- Continuous assessment of all access and actions
- Dynamic ABAC, RBAC, and PBAC access rules for all resource
- Granular least privilege access control based on roles, attributes, and just-in-time approval
- Enforce contextual access policies in real time.
- Onboard and offboard employees with just a few clicks
- Instantly grant and revoke just-in-time access to databases, servers, clusters, web apps, and cloud
- Temporarily approve elevated privileges for sensitive actions within Slack, MFST Teams or PagerDuty

Audit

Monitor and log every single event

- Realtime event monitoring for audit events
- Capture and record all the precise details of every single session, query, and command across your entire stack
- Replays available for SSH, RDP, and Kubernetes sessions
- Centralize all audit logs in one place (e.g., single unified query log across all DBMs)
- Automatically stream logs into the S3 bucket, SIEM/SOAR of your choice
- Evaluate access implementation with comprehensive reports showing user and resource utilization of all access grants

Natively supported infrastructure

These are just some of the resources we support. You can check out the complete list here.

Cloud service providers	Databases	Containers	Servers
aws	+30 MORE		

Logging	SIEM	Identity providers/SSOs	Configuration management
	sumo, syslog-ng		

Secrets management	Workflow	Message queues	Endpoint Security
AND MORE	servicenow		CROWDSTRIKE