strongdm

StrongDM™ Dynamic Access Management (DAM) Platform

Simple, secure, and dynamic access to every resource in your infrastructure

PRECISE CONTROL

Protect your resources with a unified solution that gives people just-right access every time.

FOR EVERYTHING IN THE MODERN STACK

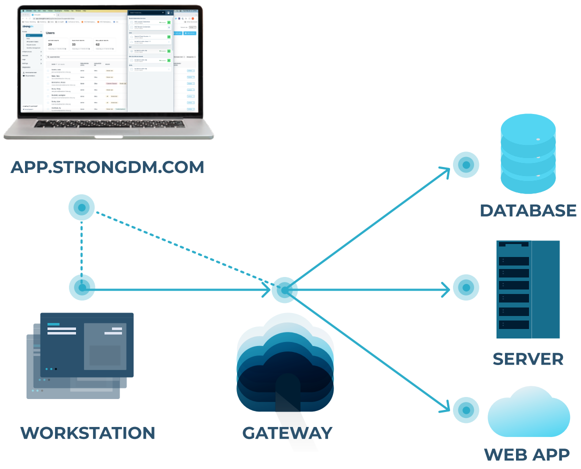
Works with your past, present, and future infrastructure, regardless of protocol or location.

WITH COMPLETE VISIBILITY

Get total visibility into everything that was authorized and executed and easily answer the who, what, where, and when.

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, and JIT access support
- Native SSO integrations, including SCIM
- REST API & fully supported SDKs in Go, Java, Python, Ruby
- Fully configurable, encrypted log storage
- Eliminate credential exposure to end users
- Robust reporting

To learn more about StrongDM or to sign up for a demo, visit www.strongdm.com strongdm

Key Capabilities

Every service you need to manage and audit access.

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

Authorization

Specify what and how much staff can access

- Dynamic ABAC & RBAC access rules for all resource
- Granular least privilege access control based on roles, attributes, and just-in-time approval
- 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 operations within Slack, MFST Teams or PagerDuty

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

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 SIEM of your choice
- Automate evidence collection for various audit regimes (e.g., SOC 2, SOX, ISO 27001, HIPAA)

Natively supported infrastructure

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

Cloud service providers

Databases

+30 MORE

Containers

Servers

Logging

SIEM

Identity providers/SSOs

Configuration management

Secrets management

AND MORE

Workflow

Message queues

And more

To learn more about StrongDM or to sign up for a demo, visit www.strongdm.com