strongdm

The Infrastructure Access Platform

strongDM delivers simple, secure access to every resource your technical staff needs.

ONE PLATFORM

Unify infrastructure access workflows with a single solution for zero-friction connectivity to everything in your stack.

FOR EVERY ENVIRONMENT

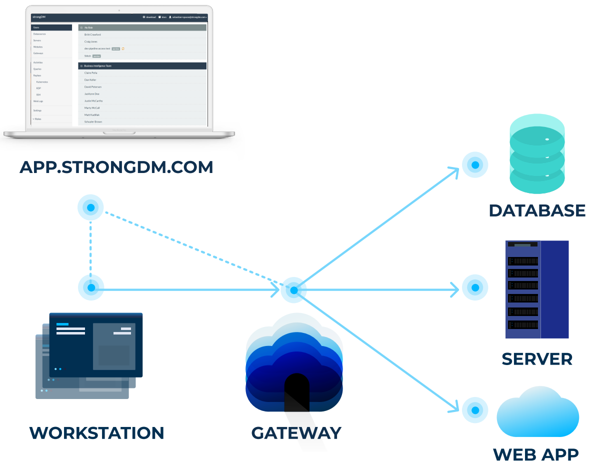
Works with your past, present, and future infrastructure, regardless of protocol or location.

DELIVERED AS CODE

Admins manage access ‘as code’, so it’s easy, flexible, and as ephemeral as your infrastructure.

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 an infrastructure access platform

Table stakes for supporting a modern stack.

- Configurable credential leasing backed by credential vaults
- Complete protocol support for SSH, RDP, K8s, & DB workflows
- No additional software deployed to your servers.
- Full auditability & replay of all supported protocol sessions
- Full granular RBAC support
- Native SSO integrations, including SCIM
- Temporary credential provisioning for on-demand access grants
- REST API & fully supported SDKs in Go, Java, Python, Ruby
- Fully configurable, encrypted log storage
- 24/7/365 support

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

Key Capabilities

Authentication

Determine who gets access to your infrastructure

- Integrate with identity providers to centrally manage infrastructure access
- Automate user & group provisioning with a single source of truth
- Store credentials securely with strongDM or use an existing secrets manager (HashiCorp Vault, AWS Secrets Manager, GCP Secret Manager)
- Native MFA integration
- Full SCIM 2 provisioning for users and roles
- 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 resources
- Granular least-privilege access control based on roles, attributes, and just-in-time approvals
- Onboard and offboard employees with just one click
- Instantly grant and revoke just-in-time access to databases, servers, clusters, web apps, and clouds
- Temporarily approve elevated privileges for sensitive operations within Slack 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

Observability

Monitor and log every single event

- Real-time 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 DBMSs)
- 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***.

Servers	Databases +30 MORE	Identity providers/SSOs	SIEM
Secrets management	Configuration management	Containers	Logging
Workflow	Message queues	Caches	Search indexes

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