Universal Privileged Access Authorization

Tech Datasheet

Secure access to any infrastructure: cloud, hybrid, or on-prem. With the industry's first Runtime Authorization.

Access at the Speed of Development

Enable secretless, frustration-free access that integrates natively into your workflows (CLI, IDEs, CI/CD).

Prevent Breaches in Real-Time

Move beyond static permissions. Enforce policy at runtime to stop lateral movement and risky commands instantly.

Continuous Compliance

Policy-based action control ensures real-time, verifiable Zero Trust compliance with comprehensive audit trails.

PLATFORM OVERVIEW

Legacy PAM secures the vault; StrongDM secures the session. Our Universal Privileged Access platform unifies authentication and runtime authorization across your entire stack, closing the gap where breaches happen.

KEY CAPABILITIES

Unlike legacy PAM solutions that force a "rip and replace," StrongDM meets you where you are in your digital transformation.

Unified Policy Control Plane

- Standard-proven Cedar-based policy language enables distributed enforcement of centralized policies.
- Write once, enforce everywhere. Manage policy for infrastructure, cloud, and agents from a single control plane.
- Sub-millisecond policy evaluation for real-time authorization decisions.
- Write once, enforce everywhere across your entire infrastructure.
- Context-aware policies using device posture, geo-location, time, and user attributes.

Continuous Runtime Authorization

- Monitor every query and command. It doesn't just check credentials at the door; it enforces policy throughout the entire session.
- Monitoring of access and operations across your infrastructure.
- Dynamic validation of user actions with adaptive security policies.
- Immediate blocking or additional verification for activities that pose security risks.
- In-session control over every action with full visibility across your stack.

Just-in-Time (JIT) Access

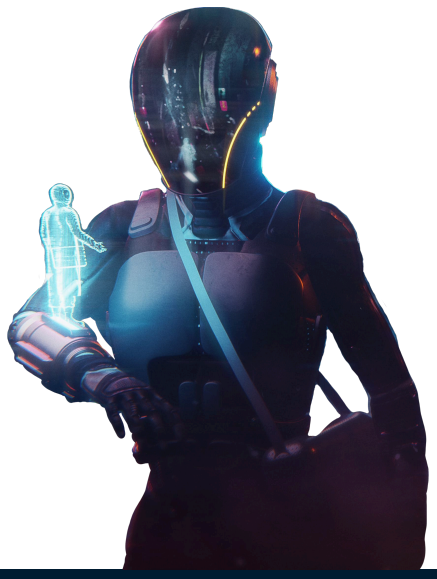
- Eliminate standing privileges with on-demand access provisioning and ephemeral credentials.
- Approval workflows with configurable justification requirements.
- Time-bound access that automatically expires.
- Integration with identity providers for seamless access revocation.

Context-Aware Enforcement

- Policies aren't just static roles. They adapt in real-time based on risk context.
- Define permissions at granular levels: who can access what and what they can do.
- Policy-based action control for databases (e.g., read-only vs. full access).
- Role-Based (RBAC), Attribute-Based (ABAC), and Policy-Based (PBAC) access control.
- Block or require MFA for specific commands or queries in real-time.

Complete Visibility & Session Management

- Comprehensive logging of every query, command, and session across all protocols.
- Monitor every interactive session across SSH/RDP/k8s.
- Activity monitoring with structured activity logs
- Export to SIEM, streaming to AWS S3, and API access to audit data



Infrastructure Support (100+ Protocols)

Category	Supported Technologies
Databases	PostgreSQL, MySQL, MongoDB, Oracle, Microsoft SQL Server, Snowflake, Amazon RDS/Redshift/DocumentDB, BigQuery, Cassandra, CockroachDB, Elasticsearch, Redis, DynamoDB, MariaDB, Teradata, ClickHouse, and more
Servers	Linux (Ubuntu, CentOS, RedHat, Debian, Fedora, Amazon Linux), Windows Server (RDP), SSH-based access for all Unix/Linux systems
Containers	Kubernetes (native), Amazon EKS, Google GKE, Azure AKS, Docker, OpenVZ
Cloud Providers	AWS (including GovCloud), Google Cloud Platform, Microsoft Azure
Network Devices	Cisco, Juniper, Palo Alto Networks, Fortinet/Fortigate, Arista

Security Stack Integrations

Integration Type	Supported Solutions
Identity Providers	Okta, Microsoft Entra ID (Azure AD), Google Workspace, OneLogin, Ping Identity, Auth0, SAML, OIDC, LDAP, ADFS
Native Vault	StrongDM Vault
Secret Management	HashiCorp Vault, AWS Secrets Manager, Azure Key Vault, GCP Secret Manager
Legacy Integration	CyberArk PAM, CyberArk Conjur, Delinea Secret Server
SIEM & Logging	Splunk, Datadog, Sumo Logic, LogRhythm, Graylog, Elastic Stack, AWS CloudWatch, Azure Monitor, Papertrail
Workflow & ITSM	ServiceNow, Jira, Slack, Microsoft Teams, PagerDuty
Endpoint Security	CrowdStrike, SentinelOne, Microsoft Defender (Device Trust)
DevOps & IaC	Terraform, Ansible, Puppet, Chef, Jenkins, GitHub Actions

KEY DIFFERENTIATORS

Agentless Architecture	No agents required on target resources, reducing complexity and attack surface.
Deploy in Hours, Not Months	Layer on top of existing stack with no migration or code changes required.
Protocol-Aware Proxy	Native understanding of database queries, SSH commands, and API calls for granular control.
Legacy + Modern Support	Unified access strategy across cloud, hybrid and on-prem infrastructure.
Zero Standing Privileges	Users never have passwords, SSH keys, or credentials; access is fully managed.
Daily Updates Without Downtime	Continuous platform improvements without service interruptions.
SCIM Support	Automated provisioning and lifecycle management integration with IdPs.

PRICING PLANS

Essentials

For teams looking to reduce access risk, stay compliant, and streamline access management.

Enterprise

For organizations with mature, complex tech stacks requiring enhanced access and action control.

GovCloud

Universal Privileged Access Authorization for regulated workloads running in AWS GovCloud.

FEATURE COMPARISON

Feature	ESSENTIALS	ENTERPRISE	GOVCLOUD
Support for 100+ Protocols	✓	✓	✓
Federated Identity/SSO (Okta, Azure AD, Google)	✓	✓	✓
Multi-Factor Authentication	✓	✓	✓
Ephemeral Credentials	✓	✓	✓
Just-in-Time (JIT) Credentials	✓	✓	✓
Access Request Workflows	✓	✓	✓
Structured Activity Logs	✓	✓	✓
SSH/RDP/Kubernetes Session Replays	✓	✓	✓
Data/Log Exports	✓	✓	✓
Cloud-Native Vault Support	✓	✓	✓
StrongDM Vault		✓	✓
Context-Based Policies		✓	✓
Device Trust Integration		✓	✓
Legacy Vault Support (CyberArk, Delinea)		✓	✓
Slack/Teams/ServiceNow/Jira Integration		✓	✓
Reports Library		✓	✓
Log Streaming to AWS S3		✓	✓
Audit API Access		✓	✓
Data/Log Retention	**30** Days	**13** Months	**13** Months

COMPLIANCE & REGULATORY SUPPORT

StrongDM helps organizations achieve and maintain compliance with comprehensive audit trails and automated evidence collection:

- SOC 2 Type II
- HIPAA
- PCI DSS 4.0
- ISO 27001
- NIST 800-53
- FedRAMP (via GovCloud)
- CISA Zero Trust Maturity Model
- NIS2
- NYDFS Cybersecurity Regulation

ABOUT STRONGDM

StrongDM is the privileged authorization company. We provide security teams with complete coverage and developers with instant access by authorizing every action in real time, not just at login.

GET STARTED

Stop managing vaults. Start managing access. Learn more about how StrongDM can secure access for your business: