

Liquibase Secure vs Liquibase Community

	Liquibase Community	Liquibase Secure
	Self-managed	Liquibase managed, tested, and supported
OPERATIONAL OWNERSHIP		
Drivers & extensions	Self-managed	Liquibase managed & tested
Testing & compatibility	Self-managed	Liquibase tested
Security patching	Self-managed	Liquibase managed
Security SLAs	None	✓
PLATFORM CAPABILITIES		
Change Automation	None	✓
Change Governance	None	✓
Change Intelligence	None	✓
Enterprise support	None	✓
Professional Services	None	✓

	65+ Database Types and Modern Database Platforms Covered	
Explore the key differences between Liquibase Secure and Liquibase Community, along with a comprehensive comparison of their features.	Liquibase Community For developers who want freedom and flexibility to manage database change on their own terms.	Liquibase Secure For enterprises that need speed with enterprise controls for governance, security, and compliance, where every driver, extension, and policy is already tested and packaged.

Change Automation			^
Liquibase MCP for Changelog Generation Generates changelogs from natural language requests through the Liquibase MCP server. Output includes rollback logic and database-specific syntax.	Not available	✓	
Deployment Connectors Runs governed database deployments from ServiceNow, GitHub, Harness, and Terraform without changing how those tools are used.	Not available	✓	
Changelogs as Code Changes are authored in SQL, YAML, JSON, or XML and versioned in Git with application code. Liquibase Secure adds Flows, policy checks, and audit evidence to the same changelogs.	Basic	Advanced	
Native CI/CD Integration Runs in Jenkins, GitHub Actions, Azure DevOps, GitLab CI, and other CI/CD systems. Liquibase Secure adds policy checks, Flows, and drift detection as pipeline steps.	Basic	Advanced	
Orchestration APIs APIs that apply one database change standard across pipelines, platforms, and teams without rebuilding existing workflows.	Not available	✓	
Liquibase Secure Developer (VS Code Extension) Creates changelogs and changesets, runs operations, and applies policy checks inside VS Code.	Not available	✓	
Local Validation Runs operations and policy checks against a local database before changes are committed.	Manual	✓	
Object Support Tracks and manages changes to tables, indexes, functions, triggers, stored procedures, and other objects using each database's full feature set.	Limited	Advanced	
Workflow Automation (Flow Files) Flow files define end-to-end pipelines in YAML. Policy checks, rollback scripts, and audit logs are captured as part of each run.	Not available	✓	
Prebuilt Workflow Templates Ready-to-use Flow templates for standard pipeline stages, from pre-merge validation through rollback.	Not available	✓	

Change Governance			^
Governed AI Changes Policy checks, approvals, and evidence collection apply to every change, whether written by a person or an AI assistant.	Not available	✓	
Traceability and Audit History Records who changed what, where, and when, with history reports, structured logging, and user identity for every change.	Limited Changelog history table only; no reports	✓	
Compliance Reporting Audit trails and policy results from the pipeline are compiled into evidence for SOX, HIPAA, PCI-DSS, SOC 2, DORA, and GDPR audits.	Not available	✓	
Policy Checks and Custom Checks Built-in and custom checks evaluate each change against defined rules and block operations that fail before deployment.	Not available Manual review only	✓	
Standards Enforcement in IDE and Pipeline The same policy checks run in the developer's IDE before commit and as CI/CD pipeline steps before deployment.	Not available Manual review only	✓	
Drift Detection and Reconciliation Scheduled or triggered scans compare deployed schemas to tracked changelogs and flag out-of-band changes. Detected drift can be reconciled by updating code or rolling the change back.	Basic Manual diff between two databases	✓	
Targeted Rollback Auto-generated and custom rollback scripts revert a single changeset or a full deployment to its last known good state in one command. Applies to human and AI-generated changes.	Basic Revert the last change or roll back to a tag or date	✓	

Change Control			^
Credential Management with Secrets Manager Integrations Database credentials are read from HashiCorp Vault, AWS Secrets Manager, or other enterprise secret stores instead of changelogs or property files.	Not available Credentials stored and managed manually	✓	
Separation of Duties and Authentication Enforces separation of duties between developers, Ops, and DBAs, supports modern authentication methods, and records each action in the audit trail.	Not available Requires custom integration	✓	
Identity-Aware Controls Gates deployments through SSO, RBAC, and CI/CD access controls, and routes changes to designated approvers.	Not available	✓	

Change Intelligence			^
Unified Change Observability Reports and dashboards cover every change across every database, including deployment health, velocity, and risk trends over time.	Not available	✓	
Schema Consistency and Data Lineage Schema changes are standardized and traceable across Snowflake, Databricks, MongoDB, and 65+ database types, with lineage recorded per environment.	Manual Not supported in product	✓	
Logging and Reporting Structured logs for every change can be exported to dashboards and reports for audit, compliance, and monitoring.	Basic Changelog table only	✓	
Root Cause Analysis Failed deployments link to operation history, logs, and execution context. AI-driven analysis summarizes the failure and proposes remediation steps.	Limited CLI output and logs	✓	
Deployment Health and DORA Metrics DORA metrics and performance health are reported by department, team, pipeline, or database.	Not available	✓	
Drift Monitoring Schema drift, policy outcomes, and operational patterns are shown in one dashboard so out-of-process changes are visible early.	Not available	✓	
Pipeline View Tracks each change from development to test, staging, and production, and shows gaps, failures, and skipped steps.	Not available	✓	
Audit Evidence on Demand Compliance evidence reports are generated on request from continuously captured change history, with no manual collection.	Limited Changelog table only	✓	
Ecosystem Integrations Sends change data to SIEM, observability, and GRC systems.	Not available	✓	

Additional Benefits			^
Supply Chain Assurance Every release ships with a Software Bill of Materials (SBOM). CVE patches are delivered under an SLA.	Not available	✓	
Testing and QA Liquibase tests each release across supported databases, including regression coverage.	Basic Unit and integration tests; compatibility verified by the user	✓	
Installation and Upgrade One-step install with certified drivers, extensions, and integrations. Upgrades are guided; patches and hotfixes are SLA-backed.	Basic Unit and integration tests; compatibility verified by the user	✓	
Support SLA-backed support with technical account management.	Community Forums and GitHub	✓	
Professional Services Implementation and best practice services from Liquibase.	Not available	✓	
Vulnerability Remediation SLA Critical vulnerabilities are patched and delivered within 14 days, with proactive notification.	No SLA	✓	
Secure Docker Image The official image is signed and attested, and ships with Java, JDBC drivers, an SBOM, and SLSA Level 3 provenance on every build.	Not available	✓	