LEIT DATA

SECURITY POSTURE AND COMPLIANCE REPORTING FOR SNOWFLAKE

Continuous Snowflake security visibility with compliance-ready reporting

SNOWFLAKE NATIVE APPLICATION

For security, compliance, and Snowflake platform teams under rising audit pressure: assess posture continuously, map findings to major frameworks, and generate exportable evidence with actionable remediation guidance.

Scan to connect

The Problem

Snowflake is increasingly in scope for major audits and regulatory reviews, but security posture and evidence are often fragmented across teams and tools.

Many teams face the same friction:

- Manual security reviews take too long
- Compliance evidence is scattered across teams and tools
- Teams lack a consistent way to assess Snowflake posture
- Findings are hard to translate into remediation priorities
- Audit preparation is repetitive and document-heavy

The result is slower follow-up, weaker visibility into control gaps, and too much time spent assembling reporting instead of improving posture.

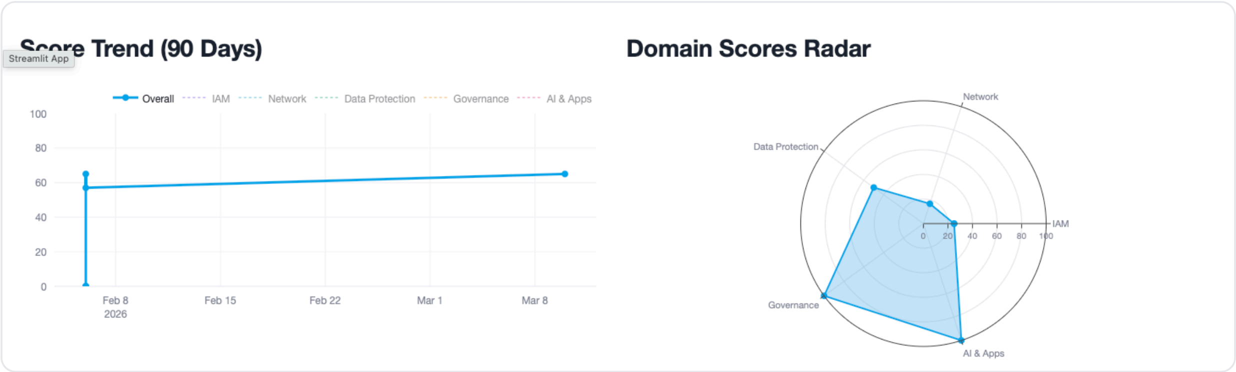
How It Works

Built as a Snowflake Native Application, the package provides a repeatable operating flow rather than a one-off audit exercise.

1. **Deploy and scan:** run posture checks across identity, network, data protection, governance, AI/native apps, and monitoring domains.
2. **Assess and prioritise:** review findings by severity and trend to focus teams on material risk first.
3. **Map and communicate:** connect technical findings to framework controls for compliance and leadership visibility.
4. **Remediate and verify:** apply SQL-oriented guidance and track follow-up progress.
5. **Export evidence:** generate evidence packs and markdown outputs for audit and internal review.

> *Scenario example: manual Snowflake security reviews often consume 2-3 weeks of analyst time per audit cycle before findings are consolidated and mapped for stakeholders.*

> *From manual reviews and scattered evidence to repeatable Snowflake security assessment, compliance mapping, and exportable reporting.*



Security Domains and Framework Coverage

Six domains and 21 controls mapped to 8 compliance frameworks.

6 Domains → 21 Controls → 8 Frameworks

Domains

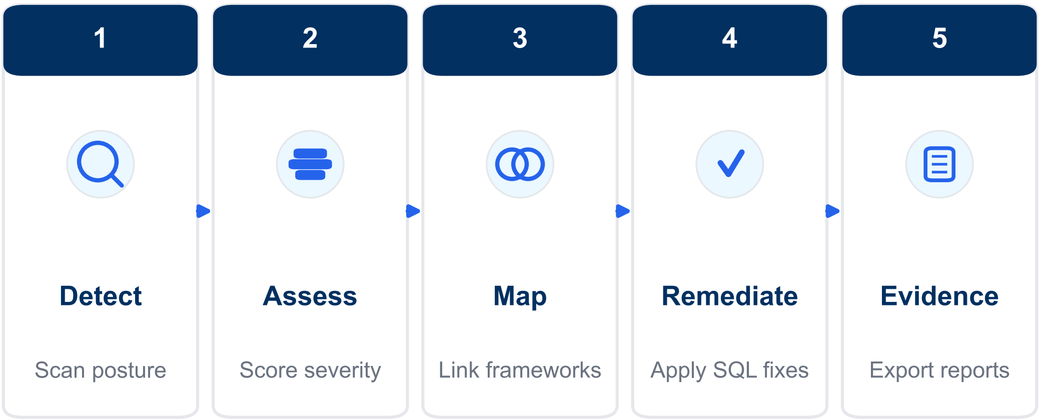
- Identity & Access
- Network & Perimeter
- Data Protection
- Governance
- AI / Native Apps
- Monitoring & Logging

Frameworks

- SOC 2
- ISO 27001
- GDPR
- NIST 800-53
- CIS v8.1
- DORA
- HIPAA
- PCI-DSS

Security Remediation Workflow

From detection to audit-ready evidence in five repeatable steps.



1 Detect — Scan posture

2 Assess — Score severity

3 Map — Link frameworks

4 Remediate — Apply SQL fixes

5 Evidence — Export reports

From findings to audit-ready evidence in one repeatable flow.

Four Ways It Creates Value

The package delivers value across four pillars: continuous visibility into Snowflake security posture, compliance-ready reporting that maps findings to frameworks, actionable remediation with prioritisation and guidance, and a native Snowflake experience that fits existing workflows.

Pillar	Outcome
Continuous Security Visibility	Gives teams an ongoing view of posture instead of relying on point-in-time reviews.
Compliance-Ready Reporting	Connects technical findings to recognised frameworks so risk can be communicated in business and audit terms.
Actionable Remediation	Supports prioritisation with category and severity breakdowns plus prescriptive SQL-based fixes and recommendations.
Native Snowflake Experience	Fits into Snowflake's operational model with Snowflake-native context and workflows.

Who It Is For

- **Security teams** - Focus on visibility into control gaps, severity-based prioritisation, repeatable assessment workflows, and remediation guidance.
- **Compliance teams** - Focus on framework mappings, evidence packs, audit readiness, and executive reporting outputs.
- **Snowflake admins** - Focus on practical findings, SQL-based remediation, native fit within Snowflake workflows, and configuration visibility.
- **Leadership** - Focus on improved visibility, reduced manual reporting effort, clearer risk communication, and faster readiness for internal and external reviews.

Why This Solution

> *Not a generic security overlay—Snowflake-native package for operational security and compliance workflows.*

The LEIT Security Package is purpose-built for Snowflake and combines posture assessment, compliance mapping, evidence generation, and remediation guidance in one package.

- Uses Snowflake-native data and security context
- Makes audit evidence generation part of the operating workflow
- Provides outputs usable by both technical and executive stakeholders
- Moves teams from manually assembled reviews to repeatable, evidence-based operations

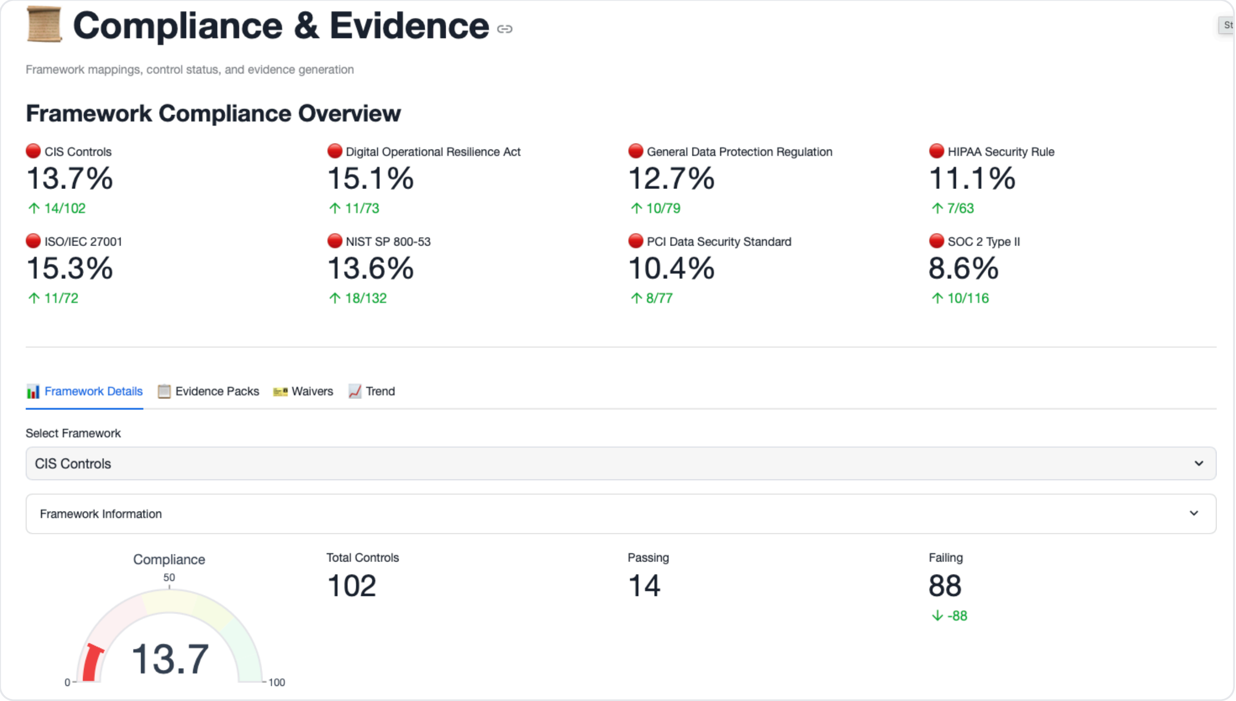
This aligns directly to **Security and Compliance**: helping organisations maintain visibility, map findings to frameworks, and produce evidence with clearer remediation guidance.

What You Get

- **Continuous posture assessment** - Ongoing view across 6 security domains and 21 security controls.
- **Framework mappings** - Coverage across 8 major frameworks with 177 total control mappings.
- **Exportable evidence packs** - Executive summaries, control mappings, findings, remediation guidance, risk ratings, and recommendations.
- **Downloadable markdown reports** - Audit and internal review outputs.
- **Actionable remediation** - SQL fixes and control-level detail so teams can prioritise and act on findings.

Security Domain	Primary Framework Coverage	Evidence Output
Identity and Access Management	SOC 2, ISO 27001, NIST	Control mapping plus prioritised remediation
Data Protection and Privacy	GDPR, HIPAA, PCI-DSS	Findings, severity, and report-ready evidence
Governance and Standards	ISO 27001, NIST, DORA	Framework alignment and gap summaries
Monitoring and Logging	CIS Controls, SOC 2, NIST	Operational findings and follow-up actions

> *Proof metrics: 6 domains, 21 controls, 8 frameworks, and 177 mappings. Teams can move from risk identification to remediation planning and audit-ready reporting without rebuilding evidence each cycle.*



Compliance & Evidence

Framework mappings, control status, and evidence generation

Framework Compliance Overview

CIS Controls	Digital Operational Resilience Act	General Data Protection Regulation	HIPAA Security Rule
13.7%	15.1%	12.7%	11.1%
↑ 14/102	↑ 11/73	↑ 10/79	↑ 7/63
ISO/IEC 27001	NIST SP 800-53	PCI Data Security Standard	SOC 2 Type II
15.3%	13.6%	10.4%	8.6%
↑ 11/72	↑ 18/132	↑ 8/77	↑ 10/116

Select Framework

CIS Controls

Framework Information

Total Controls 102

Passing 14

Failing 88 ↓ -88

Next step: Run an initial posture assessment on one Snowflake account to review current posture, framework coverage, and evidence-pack output. **Request an assessment** — www.leit-data.com/security.