

Seclore Data Security Intelligence Framework

Turn Protected File Activity Tracking into Actionable Insights

Modern enterprises need more than access logs. They need to understand how sensitive data is used, shared, and moved across teams, partners, and systems. The Seclore Data Security Intelligence Framework delivers that visibility.

What is the Data Security Intelligence Framework

The Framework transforms Seclore classification and protected file activity into clear, visual insights your teams can use to make smarter decisions.

You get a structured, queryable data model that connects directly to Power BI and other BI tools—so you can see your data security posture at a glance.

Benefits Across the Organization

As data movement increases through AI tools, cloud workflows, and human collaboration, understanding how data is used becomes essential.

The Framework gives you the visibility to:

- Reduce risk
- Strengthen compliance
- Improve operational decision-making
- Demonstrate data protection maturity

See How Your Sensitive Data Moves

Track how protected files move inside and outside the organization, including:

- Who accessed them
- What actions were taken
- When usage patterns shift
- Where files travel
- How controls perform during real collaboration

This gives security, compliance, and business teams a shared view of exposure and control effectiveness.

How It Works

- Seclore-protected files generate detailed activity telemetry.
- The Framework ingests this telemetry into a structured data model.
- Data is exposed through pre-built and custom BI dashboards.
- Optional export to your own data lake enables advanced analysis.

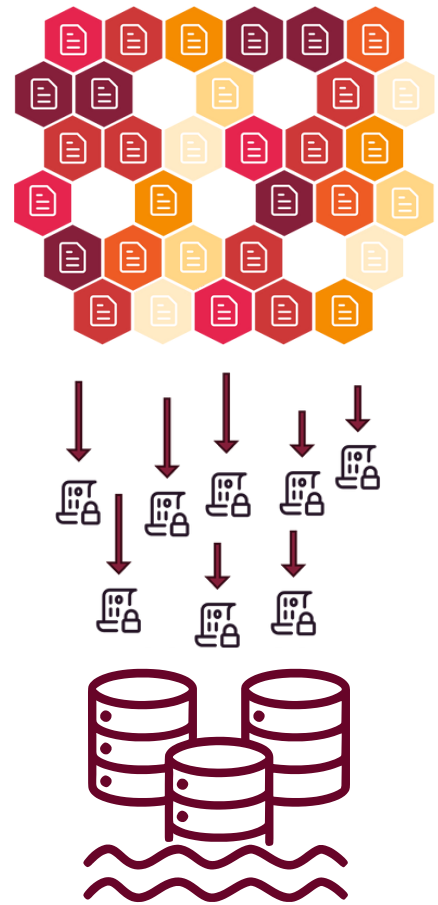
Pre-Built & Custom Dashboards

The Framework includes Power BI dashboards for:

- Enterprise Risk Insights
- Usage & Utilization
- Third-Party & Supply-Chain Exposure

Dashboards include time-series analysis, drill-downs, alerts, PDF/Excel export, and subscription options.

Build custom dashboards or enrich the data with additional business context in your own data lake.



Security Teams

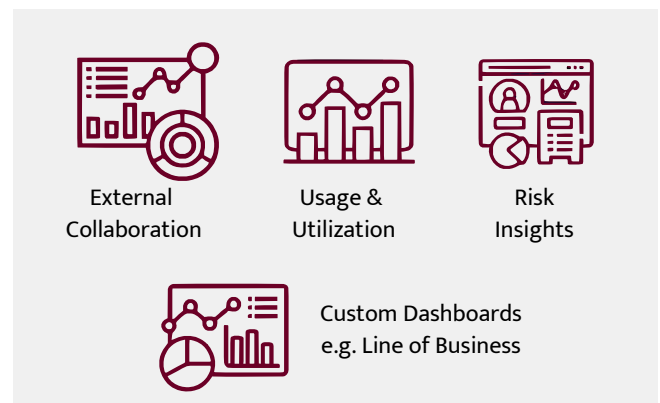
- Identify high-risk collaboration quickly
- Validate access decisions with evidence
- Reduce investigation time with clear activity trails

Compliance Teams

- Prove control effectiveness
- Generate audit-ready evidence
- Cut manual reporting efforts

Business Teams

- Understand how sensitive data supports daily work
- See collaboration patterns
- Align decisions with security and compliance requirements



About Seclore

Seclore helps the world's largest enterprises share their most sensitive data fearlessly. Our data-centric approach to cybersecurity protects and controls data whether its inside and outside of their organization. Learn why leading enterprises like American Express, Ford and IDFC Bank choose Seclore to prevent data theft and achieve compliance without sacrificing seamless collaboration and data sharing.