imperva
a Thales company

DATA SECURITY FABRIC

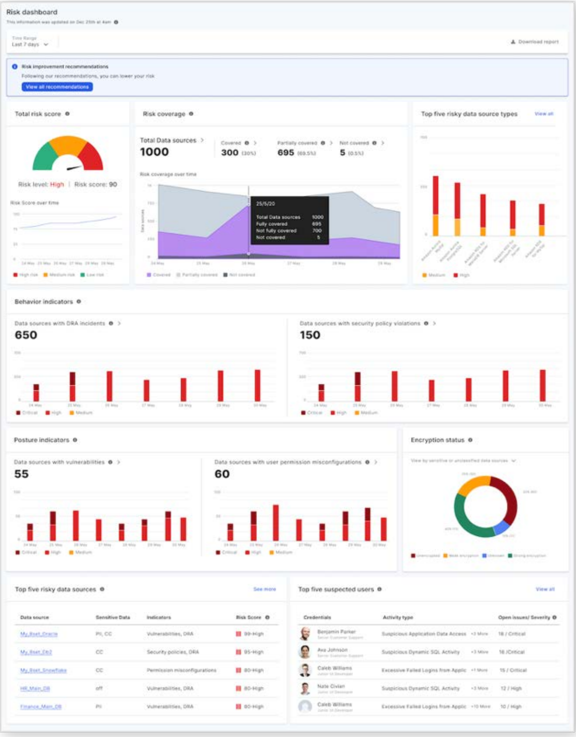
Data Risk Intelligence

Effectively Manage Data Risk and Compliance Through Comprehensive Insights and Actions

Data Security Fabric (DSF) Data Risk Intelligence empowers CIOs, CISOs, and data risk specialists to accurately pinpoint the most critical data risks by severity and likelihood, enabling them to effectively prioritize risk mitigation. It delivers specialized insights derived from a wide-ranging set of data risk indicators through advanced analytics, encompassing user permissions, data source vulnerabilities, encryption status, suspicious activities, and an all-encompassing organizational risk factor. Following this thorough analysis, DSF Data Risk Intelligence furnishes clear-cut recommendations for necessary action.

Consider this scenario: If a data source has known vulnerabilities, stores unencrypted sensitive data, and is targeted by a malicious actor, DSF Data Risk Intelligence will assign it a high-risk score. This will prioritize it at the top of the alert list and provide detailed actions to address the risk. Concentrating on insights from the complete set of data risk indicators enhances confidence in risk management efforts.

It focuses on identifying suspicious users, access, and actions in order to quickly pinpoint the most significant potential risks. Security teams receive valuable insights and trends that empower them to take prompt action or conduct further investigations with the relevant departments, including legal, compliance, and HR, to mitigate these risks. This helps in better management of data risks, ensuring accurate reporting, and addressing potential configuration drifts in risk scoring.



Risk dashboard

Time Range: Last 7 days

Risk improvement recommendations

Following our recommendations, you can lower your risk

Total risk score — Risk level: High | Risk score: 90

Risk coverage — Total Data sources 1000; Covered 300 (30%); Partially covered 695 (69.5%); Not covered 5 (0.5%)

25/5/20: Total Data sources 1000; Fully covered 695; Not fully covered 700; Not covered 5

Behavior indicators — Data sources with DRA incidents 650; Data sources with security policy violations 150

Posture indicators — Data sources with vulnerabilities 55; Data sources with user permission misconfigurations 60

Top five risky data sources

Data source	Sensitive Data	Indicators	Risk Score
My_Bset_Oracle	PII, CC	Vulnerabilities, DRA	99-High
My_Bset_Db2	CC	Security policies, DRA	95-High
My_Bset_Snowflake	CC	Permission misconfigurations	80-High
HR_Main_DB	off	Vulnerabilities, DRA	80-High
Finance_Main_DB	PII	Vulnerabilities, DRA	80-High

Top five suspected users

Credentials	Activity type		Open issues/ Severity
Benjamin Parker	Suspicious Application Data Access	+3 More	18 / Critical
Ava Johnson	Suspicious Dynamic SQL Activity	+3 More	16 /Critical
Caleb Williams	Excessive Failed Logins from Applic	+1 More	15 / Critical
Nate Civian	Suspicious Dynamic SQL Activity	+3 More	12 / High
Caleb Williams	Excessive Failed Logins from Applic	+10 More	10 / High

- Identify data risk based on the highest severity and likelihood.
- Prioritize risk mitigation based on a comprehensive range of data risk indicators.
- Get best-practice recommendations to take appropriate action.

Gain Visibility, Transparency, and Context

DSF Data Risk Intelligence offers transparency and context into your data risk status by consolidating data risk metrics, locating risk areas, and providing transparent and customizable risk scores. Additionally, it includes data encryption, risk posture management, and behavioral analytics metrics to provide context. Table 1 below provides an example of the source of context.

Table 1: Sources of Context

Encryption	Data Risk Posture	Behavior Analytics
Encryption Status of Data Store • Unavailable • Unencrypted • Weak encryption • Strong encryption	**User Right Management** ▪ User/roles ▪ Entitlement ▪ Granular data objects ▪ United cross-database reporting **Entitlement Assessment** ▪ Users ▪ Entitlements **Data Repositories Vulnerability Assessment** ▪ Log-type data sources ▪ On-premises & cloud	**Data Risk Analytics** ▪ Data context user behavior ▪ Intrusion detection ▪ Early-stage detection ▪ Unified detection **Customized Data Detection** ▪ Organization-specific detection models

Align Risk Scores to Your Organization

To make effective data risk decisions, it is vital to have an accurate risk score that reflects your specific security tolerance and organizational goals. With DSF Data Risk Intelligence, you can align the organizational risk score to your specific environment and customize it by amplifying specific databases that you consider mission-critical or that contain sensitive or PII data. You can further customize your risk score, allowing you to accurately represent the risk associated with specific high-importance databases by adjusting the weight of specific indicators, including posture, behavior, and database importance indicators.

Unified View of Risk Management

A centralized view empowers executives and data experts to make better risk management decisions and gain valuable insights.

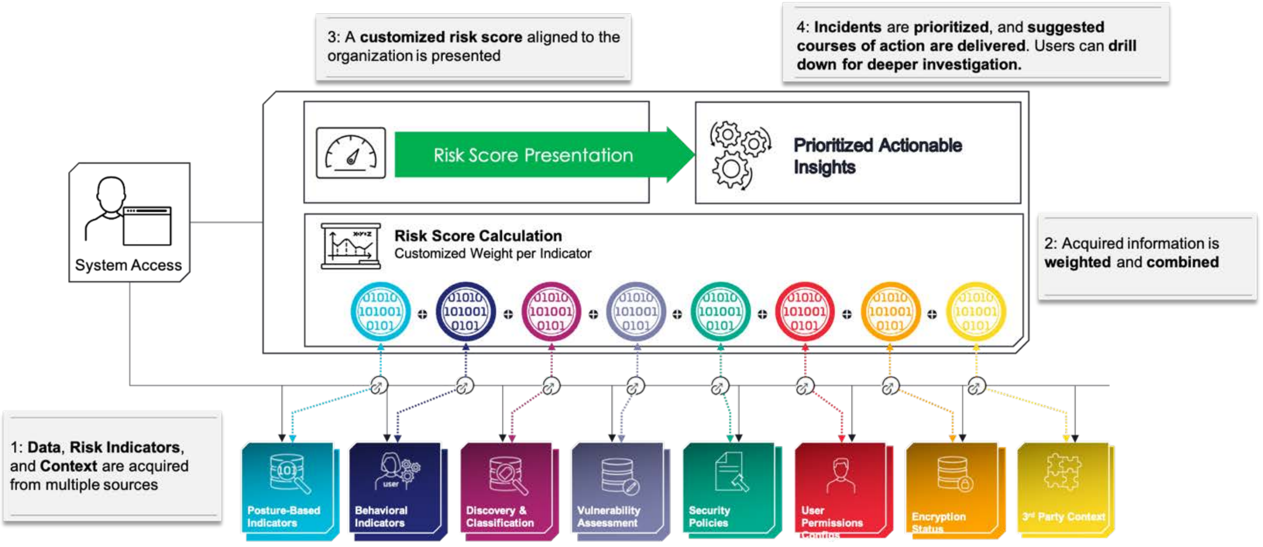
Executive View	Data Expert View
▪ Overall organization risk status that includes risk score and trends ▪ Risk indicator trends ▪ Top data sources and users at risk	▪ List of data sources prioritized for response by risk score ▪ Link to in-depth data source risk analysis ▪ Organization posture recommendations

Key Features and Benefits

Technical Feature	Benefit
Unified Risk Management Console	Executives and Data Experts can conduct discussions based on reliable data risk intelligence and insights.
Risk Management Data from Throughout Your Environment	Combine posture and behavioral parameters to create a risk score that aligns with your business and risk tolerance, giving you clear insight into where to focus your resources.
Automated Prioritization and Mitigation	Shorten the data risk management lifecycle with the power to take effective action to remediate incidents.
Transparent, Flexible, and Customizable Risk Scoring	Adjust the weight of individual behavior, posture, and important risk factors and amplify incidents from sensitive or highly important data stores for a risk score that directly aligns with your specific environment.

Business Value	Benefit
Know where to focus your efforts	Ease the day-to-day activities with precise, prioritized, and actionable insight that eases the day-to-day work.
Effectively leverage your resources	Protect data with fewer resources by unifying all data risk information and context.
Boost the skills of the team	Delegate workloads to less experienced security experts with Imperva DSF bridging the gap.
Lower operational costs – Improve ROI	Increase existing resources' productivity, efficiency, and accuracy to meet growing risk management demands.

Delivering Highly Accurate Risk Scoring



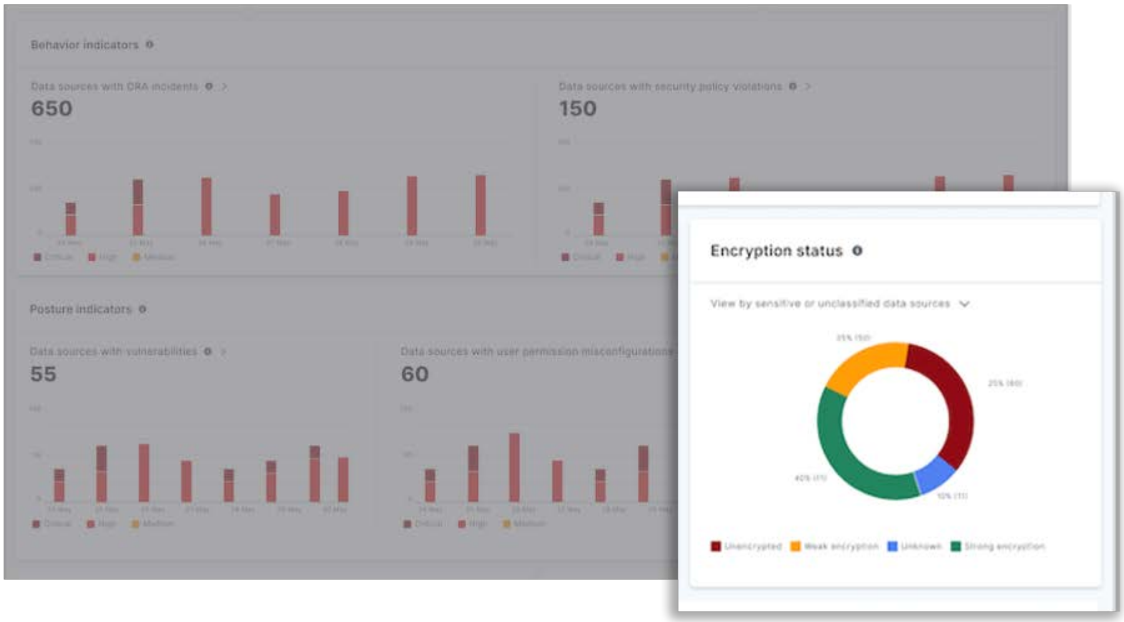
3: A **customized risk score** aligned to the organization is presented

4: **Incidents** are **prioritized**, and **suggested courses of action are delivered**. Users can **drill down for deeper investigation.**

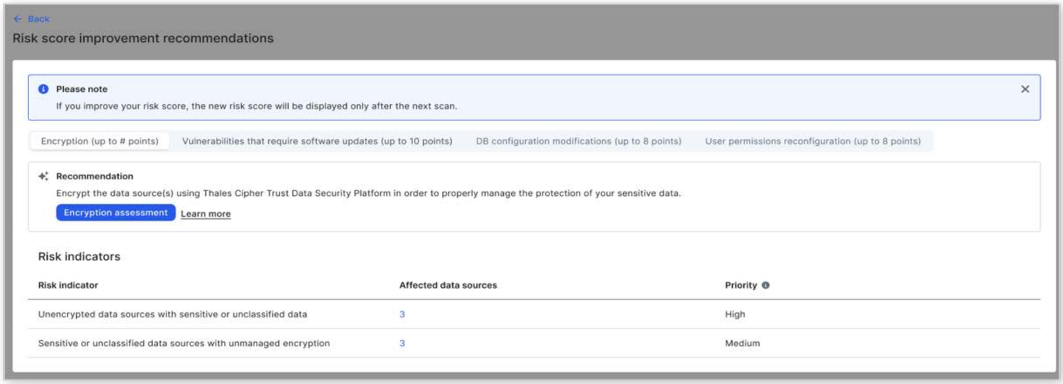
2: Acquired information is **weighted** and **combined**

1: **Data, Risk Indicators,** and **Context** are acquired from multiple sources

An organization-wide risk score and well-prioritized tasks help minimize risk in the organization.


Behavior indicators
Data sources with DRA incidents
650
Data sources with security policy violations
150
Critical
High
Medium
Posture indicators
Data sources with vulnerabilities
55
Data sources with user permission misconfigurations
60
Encryption status
View by sensitive or unclassified data sources
25% (50)
25% (60)
40% (11)
10% (11)
Unencrypted
Weak encryption
Unknown
Strong encryption

Views of behavior and posture trends showing encryption status .



Risk score improvement recommendations

Please note

If you improve your risk score, the new risk score will be displayed only after the next scan.

Encryption (up to # points) | Vulnerabilities that require software updates (up to 10 points) | DB configuration modifications (up to 8 points) | User permissions reconfiguration (up to 8 points)

Recommendation

Encrypt the data source(s) using Thales Cipher Trust Data Security Platform in order to properly manage the protection of your sensitive data.

Risk indicators

Risk indicator	Affected data sources	Priority
Unencrypted data sources with sensitive or unclassified data	3	High
Sensitive or unclassified data sources with unmanaged encryption	3	Medium

Recommend encrypting data sources with Thales Cipher Trust Security Platform for any data source with sensitive data/without classified data or strong encryption.

About Imperva

Imperva, a Thales company, is the cybersecurity leader that helps organizations protect critical applications, APIs, and data, anywhere, at scale, and with the highest ROI. With an integrated approach combining edge, application security, and data security, Imperva protects companies through all stages of their digital journey. Imperva Threat Research and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy, and compliance expertise into our solutions.

This document is being provided for INFORMATIONAL PURPOSES ONLY. The information provided represents Imperva's point of view as of the date this document was prepared. Imperva undertakes no obligation to update or revise this information. The information should not be construed as a commitment to deliver any specific solution, upgrade, feature, or functionality.