Informatica Secure@Source

Key Benefits

- Powerful analysis and visualisations of sensitive data by function, geography, cost, and policy for audit and governance
- Accelerate GDPR compliance with data classification policies for the identification, risk analysis, and remediation of GDPR assets
- Continuously monitor and track sensitive data risks that threaten data security, compliance, and privacy
- Support of security operations efficiency with automated orchestration of data security remediation
- Identify unusual user behaviour or data access that present risk to the organisation

Detect and protect for digital transformation.

Secure@Source helps organisations detect and protect critical data across their enterprises, lowering the risk of cloud modernisation, big data, and customer-centricity initiatives. It leverages artificial intelligence (AI) and machine learning to deliver actionable data discovery and classification, risk scoring, behavioural analytics, and automated protection in a single solution. It supports both structured and unstructured data, cloud, on-premises, and big data anywhere, as well as any relational systems.

Visibility and control of sensitive data

Secure@Source provides rich visualisations of sensitive data for management and practitioners, with an intuitive user interface and continuous risk analysis of critical-data across the enterprise. Informatica Secure@Source provides a holistic enterprise view and analysis of sensitive data assets, so that organisations can rapidly assess their data security and compliance risks. This provides the intelligence to prioritise data security and compliance investments, policies, and programs.

Secure@Source enables organisations to:

- Confirm what they know about their structured and unstructured sensitive data: Global visibility of sensitive data across cloud, big data, and on-premises data stores with data classification, discovery, proliferation analysis, user access, and activity correlation and visualisation for management and practitioners.
- Monitor risk on a continuous basis: Track sensitive data risk and remediation with risk scoring based on multiple factors that identify top risk areas based on organisational requirements.
- Uncover the unexpected: Utilising user behaviour analytics (UBA), detect suspicious or unauthorised data access by continuously correlating, base-lining, analyzing, and alerting on high risk conditions and potential anomalous behaviours that threaten sensitive data.
- Remediate risk: Automate the orchestration of data security controls to protect data at rest and in use, prevent unauthorised access, and de-identify/anonymize sensitive data.

Intelligent data discovery and risk scoring

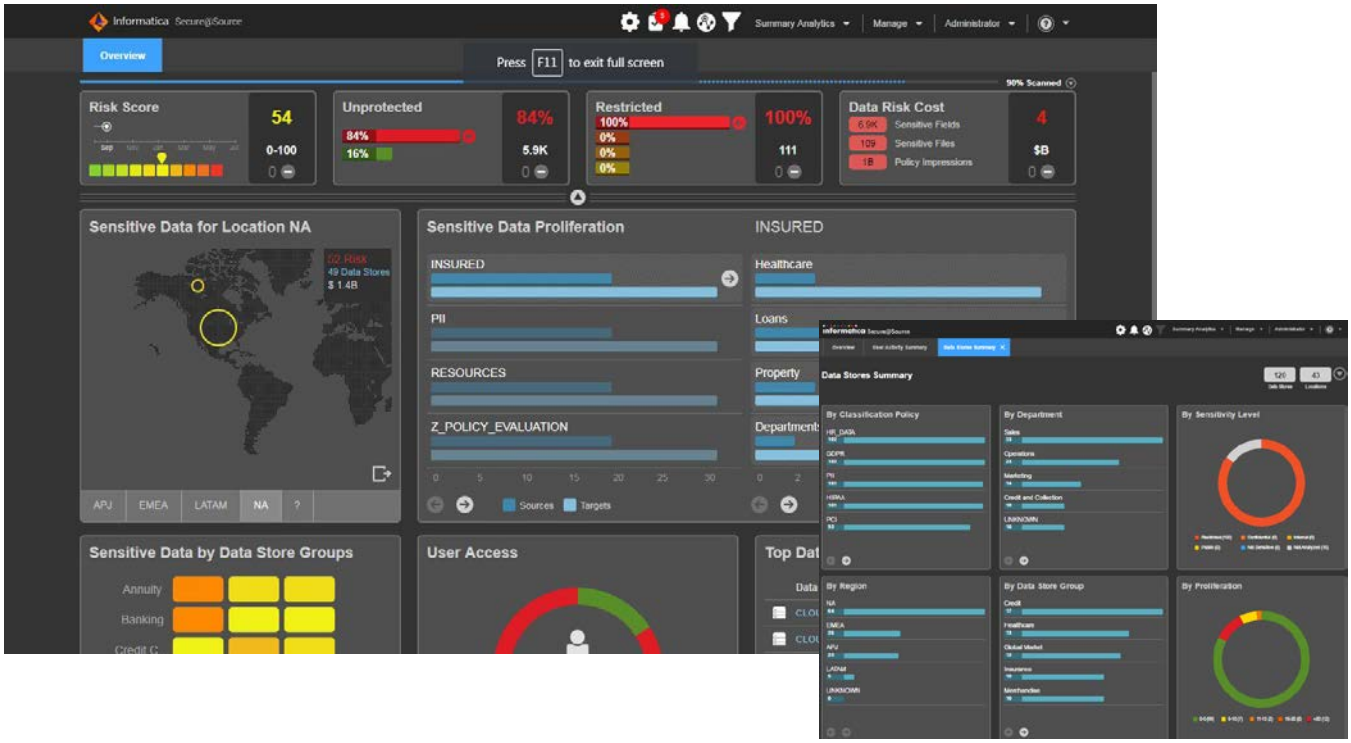
Secure@Source's data policies define data risk in context by applying a combination of data domains to define GDPR, PII, PHI, and PCI risks relevant to policies, laws, and regulations. Sensitive data discovery not only identifies location, but also provides functional and organisational information such as department, application, user, and data storage types.

Coverage includes structured data across traditional relational databases, including mainframes; semi-structured data (CSV, XML, JSON) on HDFS and Amazon S3; unstructured data on CIFS and NFS; and traditional structured data stores.

Secure@Source provides actionable risk scoring based on customisable factors, including data sensitivity, volume, protection, proliferation, location, and user activity. Risk scores can be monitored and tracked to determine the effectiveness of remediation and identify new threats.

User behaviour analytics (UBA) and user activity

Secure@Source detects anomalous user behaviours through sophisticated machine learning techniques, rules, and policies to identify activity and behaviour that could threaten data security and privacy. Secure@Source visualises anomalies in sensitive data access and movement and provides actionable intelligence of root cause and sensitive data targets.



Secure@Source provides 360-degree visibility of sensitive data through its dashboard (left) and Data Store Summary according to a variety of criteria, including sensitivity level and classification policy (right).

Key Features

Data classification and discovery

Secure@Source enables the discovery and classification of sensitive data based on data and metadata patterns and rules. From prebuilt and customisable definitions, organisations define data domains and policies to identify and locate sensitive data including GDPR, PII, PCI, PHI, and other confidential information.

Secure@Source automates the discovery of sensitive data across large numbers of databases, files stores, big data repositories, and cloud data stores. It uses flexible, high-performance, scalable scanning to uncover sensitive data and show results quickly and clearly.

Sensitive data risk analytics

The level of sensitive data risk is determined by analyzing multiple factors including protection status, user access, activity, volume, data cost, classification, and proliferation. Organisations can weight each factor according to their own risk-measurement requirements. This analysis produces risk scores that pinpoint the highest risk areas to prioritise remediation activities.

Organisations can measure the effectiveness of security investments by tracking how risk scores trend over time. Risk analytics are presented in a highly interactive and graphical visual format that enables quick identification of areas requiring attention.

User behaviour analytics, access, and activity

Unauthorised and inappropriate access to sensitive data is a major challenge in the data-driven economy. Secure@Source correlates user and user group access information from directory services, identity and access management and governance systems, and third-party and custom sources. It also analyzes user activity from databases, mainframe systems, big data repositories, and SaaS applications to provide visibility into sensitive data usage and high-risk activities.

Secure@Source detects anomalous behaviours and insider/outside threats using machine learning, rules, and policies. The combination of anomaly detection and policy-driven violations reduce alert fatigue, helping organisations prioritise and accelerate investigations as well as provide immediate and automated remediation of high-risk conditions.

Secure@Source provides holistic enterprise visibility of sensitive data through its dashboard (left) and data store summary according to a variety of criteria, including sensitivity level and classification policy (right).

Orchestration of data security controls

Security teams can remediate high risk data with the managed application of security controls on high risk data. Whether access controls, encryption, masking, or other controls, organisations can integrate risk identification and remediation for accuracy and efficiency.

Data proliferation analysis

It's critical to understand not only where sensitive data resides, but also where it's moving and being replicated to other data stores within the organisation and to cloud applications. Organisations may also want to monitor sensitive data flowing in and out of highly regulated countries or between partner and client organisations.

Secure@Source analyzes data proliferation from Informatica data flows and provides an aggregated and visual map of sensitive data proliferation, identifying sensitive data that has the greatest proliferation. Alerting of high-risk conditions Information security teams can define security policies to notify them when high risk conditions are detected, such as when a high volume of sensitive data is leaving a highly-regulated country or when unusual data access or behaviour occurs.

Visual analytics, reporting, and dashboards

Secure@Source has a rich array of dashboards that clearly presents the state of sensitive data risk to decision makers and stakeholders. The highly interactive and visual interface also lets practitioners drill down and perform detailed analyses of sensitive data risk.

Sorting information can reveal trouble areas by classification policy, location, region, department, data store, or line of business. These reports let security practitioners and decision makers share a common platform on which to base tactical and strategic analysis and decision making.

The user activity summary allows you to analyze user access to sensitive data and detect unusual activities or behaviour.

About Informatica

Digital transformation is changing our world. As the leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead the way. To provide you with the foresight to become more agile, realise new growth opportunities or even invent new things. We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption. Not just once, but again and again.

Addresses key business challenges

Intelligent data discovery and classification

Secure@Source provides complete sensitive data visibility with data classification, discovery, and risk analysis of data across the enterprise. Rich visualisations and drill-downs support both management and practitioner needs. With Secure@Source, organisations know where their private and sensitive data is proliferating—both inside and outside the enterprise and between partner and client organisations.

Intelligent data compliance

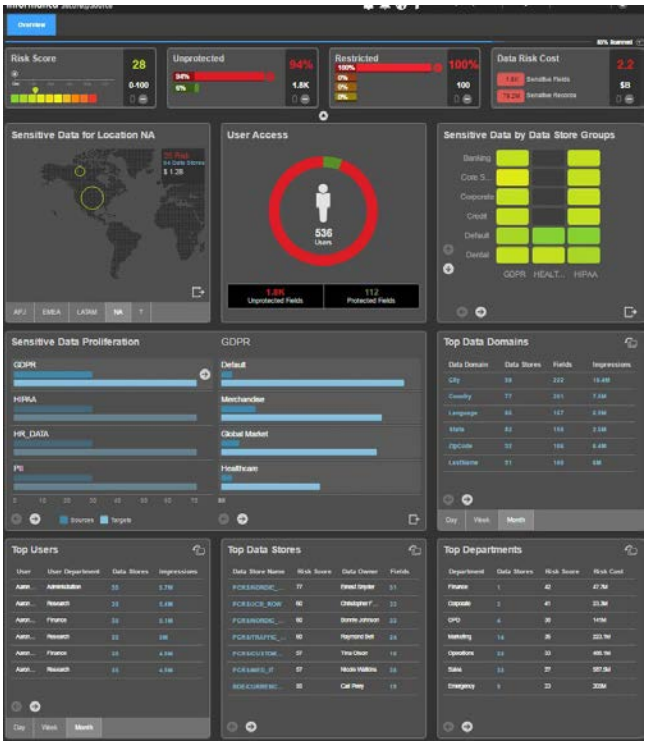
Baseline, accelerate, and continuously measure compliance of regulated data with risk scoring based on multi-factor analysis and scoring and support enforcement with automated remediation and user and data monitoring.

Intelligent data protection

Identify critical data-protection priorities, apply protection directly on the data, with automated remediation leveraging Ranger, Sentry, data masking, and encryption. Monitor and alert on user behaviour, data access, and movement.

Intelligent data audit

Accelerate audit response with detailed visualisations and reports for auditors of location, risk, protection, value, and access of regulated data. Secure@Source automates the analysis of critical data assets to support on-demand and trend reports of sensitive data risks and user activity, for data privacy, security auditing, and governance programs.



The User Activity Summary allows you to analyze user access to sensitive data and detect unusual activities or behaviour.

Informatica