Informatica Secure@Source

Key Benefits

- Continuously monitor and track sensitive data risks that threaten compliance and privacy
- Identify unusual user behavior or data access that present risk to the organization early
- Orchestrate security controls for high-risk data remediation
- Provide powerful visualizations of sensitive data by function, geography, and policy for audit and governance

Detect and Protect.

The continued escalation of data breaches, exponential data growth and proliferation, and new analytic applications and privacy laws have amplified sensitive data risk. Organizations need better visibility and control of their sensitive data across the enterprise to accurately identify, monitor, and remediate conditions that threaten it.

Visibility and Control of Sensitive Data

Secure@Source provides innovative capabilities that can improve data security and compliance, optimize security investments, and reduce sensitive data risk. It allows organizations to:

- **Confirm what they know about their sensitive data:** Global visibility of sensitive data with data classification, discovery, proliferation analysis, user access, and activity correlation and visualization 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 organizational requirements.
- **Uncover the unexpected:** Detect suspicious or unauthorized data access by continuously correlating, base-lining, detecting, and alerting on high risk conditions and potential anomalous behaviors that threaten sensitive data.
- **Remediate risk:** Orchestrate data security controls to protect data at rest, prevent unauthorized access, and de-identify/anonymize sensitive data.

Advanced Discovery and Risk Scoring

Secure@Source's data policies define data risk in context by applying a combination of data domains to define PII, PHI, and PCI risks relevant to policies, laws, and regulations across relational, cloud, and Hadoop data stores. Sensitive data discovery not only identifies location, but also provides functional and organization information such as department, application, user, and data storage types. Coverage includes semi-structured data (CSV, XML, JSON) on HDFS and Amazon S3, as well as Microsoft SQL Server Integration Servies (SSIS) proliferation information.

Secure@Source provides actionable risk scoring based on multiple 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 Behavior Analytics and User Activity

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

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 customizable definitions, organizations define data domains and policies to identify and locate sensitive data including PII, PCI, PHI, and other confidential information.

Secure@Source automates the discovery of sensitive data across large numbers of databases, 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

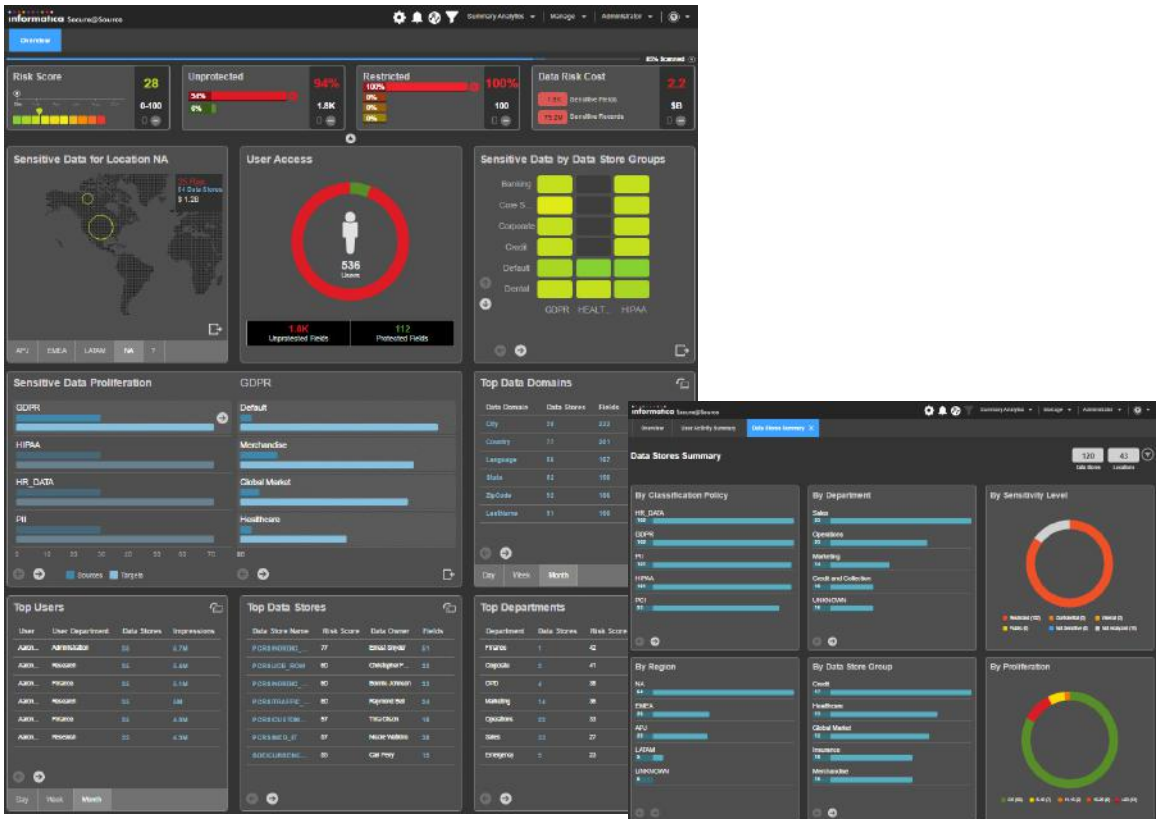
The level of sensitive data risk is determined by analyzing multiple factors including protection status, user access, activity, location, data cost, classification, and proliferation. Organizations can weight each factor according to their own risk-measurement requirements. This analysis produces risk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

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

User Behavior Analytics, Access, and Activity

Unauthorized 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 other 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 behaviors and insider/outside threats using machine learning, rules, and policies. The combination of anomaly detection and policy-driven violations reduce alert fatigue, helping organizations prioritize and accelerate investigations as well as provide immediate and automated remediation of high-risk conditions.



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).

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, organizations 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 organization and to cloud applications. Organizations may also want to monitor sensitive data flowing in and out of highly regulated countries or between partner and client organizations.

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.

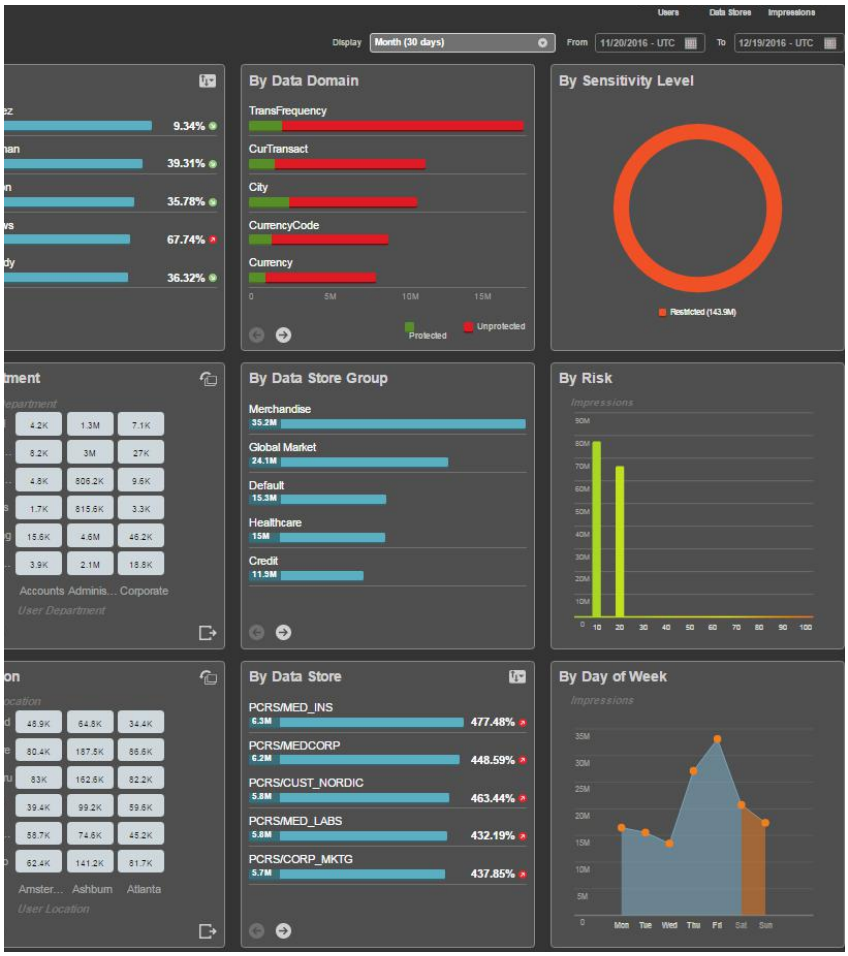
Alerting of High-Risk Conditions

Information security teams can define alert rules 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 behavior occurs.

Visual Analytics, Reporting, and Dashboards

Secure@Source has a rich array of dashboards that clearly present 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 and strategic analysis and decision making.



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

About Informatica

Informatica is 100 percent focused on data because the world runs on data. Organizations need business solutions around data for the cloud, big data, real-time and streaming. Informatica is the world's No. 1 provider of data management solutions, in the cloud, on-premise or in a hybrid environment. More than 7,000 organizations around the world turn to Informatica for data solutions that power their businesses.

Key Benefits

Alert on High Risk Conditions

Continuously correlate, baseline, detect, and alert on high risk conditions and potential anomalous behaviors or user activity.

Remediate Risk

Orchestrate and manage security controls to protect data at rest; de-identify sensitize data for test, reporting, and analytics; and implement role-based data access controls for enterprise applications.

Prioritize Security Investments

Organizations can prioritize and maximize their security investments by understanding the highest areas of sensitive data risks, measuring risks over time, and aligning their data security investments, policies, processes, and actions accordingly.

Eliminate Costly, Error-Prone Manual Efforts

Manually classifying, surveying, and reporting on sensitive data assets is costly, laborious, and error-prone. Automating these tasks lets organizations allocate resources to corrective actions and create more precise, repeatable results that improve ROI on security investments.

Streamline Sensitive Data Audit and Governance

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.

Visibility to Sensitive Data Proliferation

Tracking sensitive data proliferation lets organizations better comply with privacy laws and data usage policies. With Secure@Source, organizations know where their private and sensitive data is proliferating—both inside and outside the enterprise and between partner and client organizations.

Worldwide Headquarters, 2100 Seaport Blvd, Redwood City, CA 94063, USA Phone: 650.385.5000 Fax: 650.385.5500
Toll-free in the US: 1.800.653.3871 informatica.com linkedin.com/company/informatica twitter.com/Informatica

© 2016 Informatica LLC. All rights reserved. Informatica® and Put potential to work™ are trademarks or registered trademarks of Informatica in the United States and in jurisdictions throughout the world. All other company and product names may be trade names or trademarks.

IN06_0415_2878_1216