

Informatica Secure@Source

Key Benefits

- Protection and monitoring of personal and sensitive data to fuel data-driven digital transformation and support privacy and compliance efforts
- Visibility across all data platforms and types, providing the support needed for today's complex, hybrid environments
- Continuous risk analysis of personal and sensitive data, to prioritize resources and investments across functional, geographic, and line of business views
- AI-driven detection to uncover high-risk, anomalous data usage
- Automated orchestration and protection with sensitive data intelligence to remediate privacy and security risks

Discover, Classify, Remediate and Monitor Personal and Sensitive Data

Informatica® Secure@Source® helps you discover and remediate personal and sensitive data risk across your organization. It leverages artificial intelligence (AI) and machine learning to deliver actionable data discovery and classification, risk scoring, behavioral analytics, and automated protection in a single solution. It supports both structured and unstructured data in cloud, on premises, and big data stores, as well as any relational and mainframe systems.

Secure@Source helps you prioritize data protection and privacy investments, policies, and programs:

- **Confirm what you know about your structured and unstructured sensitive data:** Both management and practitioners gain global visibility into personal and sensitive data across the enterprise with data classification, discovery, proliferation analysis, user access, and activity correlation.
- **Continuously monitor risk:** Track data risk and remediation based on multiple factors, customizable to your organization's needs, and identify top risk areas based on requirements.
- **Uncover the unexpected:** Leverage analytics to detect suspicious or unauthorized data access by continuously correlating, baselining, analyzing, and alerting on high-risk conditions and potential anomalous behaviors that threaten sensitive data.
- **Remediate risk:** Automate the orchestration of data security controls to protect data at rest and in use, prevent unauthorized access, and de-identify/anonymize/pseudonymize sensitive data. The risk simulator helps you understand the impact of data controls before implementation.

Key Features

Locate and Classify Sensitive Data

- Locate, classify and analyze the risk of sensitive and personal data across the enterprise—in structured data across traditional relational databases, such as mainframes; semi-structured data (CSV, XML, JSON) on HDFS and Amazon S3; unstructured data on CIFS NFS; and SharePoint traditional structured data stores.
- Attain complete sensitive data visibility with dashboards and drill-downs to identify functional and organizational information such as department, application, user, and data storage types.
- Gain a complete understanding of data movement with proliferation tracking and interactive visualizations—both inside and outside the enterprise and between partner and client organizations.

About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities or create new inventions. With 100% focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

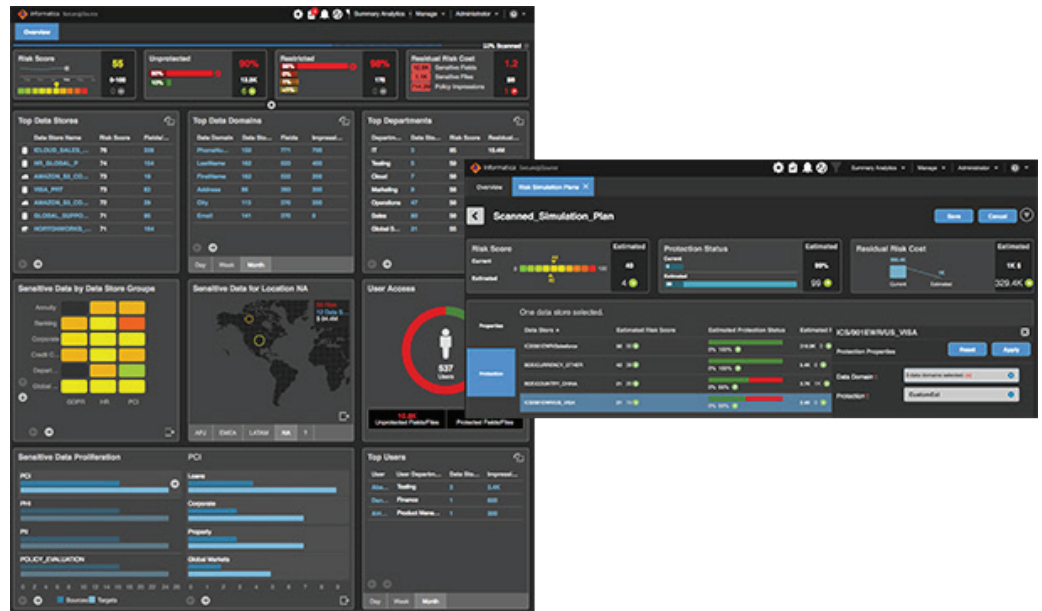


Figure 1. Secure@Source provides 360-degree visibility of sensitive data through its dashboard (left), and risk remediation simulation (right).

Ensure Regulatory Compliance

- Accelerate and continuously measure regulated privacy data compliance with risk scoring based on customizable factors, including data sensitivity, volume, protection, proliferation, location, and user activity.
- Apply a combination of data domains to define GDPR, PII, PHI, and PCI risks relevant to policies, laws, and regulations.
- Enforce compliance with automated remediation, and user and data monitoring.

Protect Sensitive Data

- Identify critical data-protection priorities.
- Protect sensitive data with automated remediation that leverages integrated Informatica Dynamic Data Masking, Persistent Data Masking, and third-party protection methods such as Hortonworks Ranger, Cloudera Sentry, and encryption.
- Integrate with custom scripts, email notifications, system log messages, or ServiceNow tickets. Configure these actions to run when triggered by security policy violations or run them manually when potential risks are detected.
- Monitor and alert on user behavior, data access, and movement.

For more information, visit the [Secure@Source Product Page](#).



Worldwide Headquarters 2100 Seaport Blvd., Redwood City, CA 94063, USA Phone: 650.385.5000, Toll-free in the US: 1.800.653.3871

IN06_0818_02878