

# Building Data-Centric Security With Informatica Secure@Source to Gain Actionable Insights Into Sensitive Data Risk

## Abstract

In February 2016, Informatica announced its release of the second version of Secure@Source, a unified platform for identifying, analyzing, and quantifying sensitive data risk. This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Impact Brief details the announcement and recognizes Informatica's innovation and leadership in the area of sensitive data risk and information security.

## Informatica Secure@Source – Managing Sensitive Data Risk

On February 16, 2016, Informatica LLC (<http://www.informatica.com>) announced the release of Secure@Source Version 2, a solution aimed at better addressing the security and data management needs of organizations through comprehensive visibility and risk management of sensitive data. Secure@Source v2 provides visibility into risk associated with data across geographic regions, users, groups, and data store access. It identifies the level of potential risk and provides a view of activities surrounding sensitive data, including who is accessing it and how it is being used. The ability to customize rules and procedures surrounding sensitive data and create alerts enhances overall risk management efforts across the organization and provides CIOs and Data Security Officers with the tools they require to manage sensitive data risk.

Informatica, a data management company, provides software to integrate, clean, transform, archive, and secure data. It is best known in the security market for its data masking products. Secure@Source is a new market-changing data security intelligence product from the company.

Founded in 1993, Informatica is headquartered in Redwood City, California. The company serves over 5800 companies worldwide in the following industries: aerospace, automotive, energy and utilities, entertainment/media, financial services, healthcare/life sciences, high technology, insurance, manufacturing, public sector, retail, services, telecommunications, and travel/transportation.

## Key Observations of Secure@Source Version 2

- **Expanded visibility into user access and activity** – Allows access to user metrics, trending activities, and event details to ensure greater visibility into sensitive data and potential risk.
- **Early-warning alerts and pre-emptive sensitive data risk management capabilities** – Dashboards, analytics, and risk management alerts provide proactive assessment and visibility into sensitive data risk.
- **Discovery for big data and SaaS-based applications** – Includes connectivity to Hadoop (Cloudera Hive) and Salesforce.
- **Customization of data domains and risk-factor scoring** – Enables flexible design and management of information and associated risk, taking into account geographic and industry-related requirements.
- **Details are available at** <https://www.informatica.com/products/data-security/secure-at-source.html#fbid=PYNn-aYbdVI>.

## EMA Perspective

Secure@Source v2 addresses a major challenge for organizations. Sensitive data presents a specific risk that expands beyond traditional security controls as organizations' information management infrastructures become more complex. Organizations need to expand the way they understand and secure their data and develop a proactive approach to manage risk associated with sensitive data. Moreover, they need to address the challenges associated with sensitive data stored within different geographical regions and logical locations. Secure@Source v2 provides an automated approach to managing sensitive data risk management, with added customization capabilities, so that CIOs, CTOs, CISOs, and other data and security professionals and stakeholders can manage this risk associated with sensitive data assets more effectively.

The ability to use analytics provides context for information surrounding sensitive data. Secure@Source lets users analyze events, trends, users, and groups and combines this information to identify who is accessing data, what groups they are a part of, and the details surrounding that access. Additionally, dashboards provide the insight into metrics and provide an overall view that can be used to ensure proactive risk management. Secure@Source highlights sensitive data risk so that organizations can take pre-emptive measures to help prevent breaches and reduce breach impact. By understanding sensitive data across the organization, organizations can target controls, processes, and policies to ensure risk reduction. This cohesive view of sensitive data provides a centralized way to manage and control access. It also supports organizations in their ability to manage privacy and security more effectively while creating parameters to ensure that any potential threats are identified before they happen.

With risk management alerts and analytics, Secure@Source provides organizations with control over their data. Based on the fact that organizations struggle with managing data security due to complex and diverse data environments, managing sensitive data effectively provides an added layer of security and helps identify areas within the data infrastructure that need to be addressed to ensure compliance and better data management. Organizations understand that they cannot overlook security and are increasingly adopting methods to secure their data, such as masking, encryption, and applying industry-supported security protocols. The reality is that all of these actions still overlook how sensitive data is handled at the source and what potential risk exists. With Secure@Source, organizations are able to ensure that their security strategy encompasses all aspects of security, including who has access to sensitive data internally, where it is stored, and what is being done with it, enhancing overall auditing capabilities over time. Being able to provide an automated approach to risk management of sensitive data increases overall operational efficiencies and, through alerts, also helps security professionals manage these requirements without having to constantly monitor how people are accessing data or what is taking place in different geographic regions.

One of the benefits of Secure@Source is that although general sensitive data domain definitions are provided out of the box, organizations can customize their data domains and create content policies that are specific to their industry and company. Organizations can create individualized rule sets for data based on varying rules for different countries and manage each data set according to where the data physically resides. Secure@Source also lets companies integrate data security-related information from other security solutions, such as user access information from LDAP/Active Directory/IAM, user activity logs from DAM solutions or databases, and asset inventories. As organizations continue to expand their reach globally, the ability to apply unique rules to different data sets and comply with geographic guidelines becomes essential. Continuous

---

*By understanding sensitive data across the organization, organizations can target controls, processes, and policies to ensure risk reduction.*

---

---

*As organizations continue to expand their reach globally, the ability to apply unique rules to different data sets and comply with geographic guidelines becomes essential.*

---

customization—combined with the overall ease of use of the system—allows businesses to take a proactive and self-service approach to enhancing their sensitive data risk management environment.

In addition to a variety of capabilities and analytics, Secure@Source v2 takes into account that organizations are increasingly leveraging cloud and big data sources. Secure@Source v2 provides the groundwork for ensuring risk management within these data sources. Support for Hadoop and Salesforce is the first step toward broader data access and increased flexibility. As more organizations try to leverage their cloud and big data infrastructures, they will require a way to manage risk and security for that data. Customer-related data and diverse access to big data sources means that more sensitive data will be stored over time. Mitigating risk means applying rules to identify risks to sensitive data and develop alerts to manage any potential risks or data access inconsistencies.

Ensuring security for sensitive data can no longer be overlooked, and organizations cannot simply develop ways to ensure that sensitive data is only secured in transit. To ensure overall data security, sensitive data needs to be managed as part of a broader security strategy supported by people, processes, and technology. Secure@Source v2 provides all of these components in an easy-to-manage interface. With risk scoring, automated alerts, analytics, and the ability to drill through to identify who is accessing data and how it is being used, organizations gain valuable insights into their sensitive data and can develop a strong framework to mitigate overall risk associated with it. Secure@Source can also be considered part of the security investment process, as it helps identify and prioritize the right places to invest in controls.

Informatica's investment in Secure@Source shows continued commitment to enhancing overall risk management and information security. Based on this, EMA recognizes Informatica as a leader in data management and security.

---

*To ensure overall data security, sensitive data needs to be managed as part of a broader security strategy supported by people, processes, and technology.*

---

### **About EMA**

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at [www.enterprisemanagement.com](http://www.enterprisemanagement.com) or [blogs.enterprisemanagement.com](http://blogs.enterprisemanagement.com). You can also follow EMA on [Twitter](#), [Facebook](#) or [LinkedIn](#).

3324.021216