



Reducing Security Risk with Courion Sensitive Data Manager

Benefits:

- Improves security – by ensuring that only the right people have the right access to sensitive data.
- Reduces risk – by providing the identity context organizations require to implement the most appropriate remediation policy.
- Streamlines business – by allowing managers to quickly and easily approve exceptions or modify alert levels where appropriate.
- Improves productivity – by highlighting sensitive data alerts that represent the highest level of risk to the organization.

As companies grow increasingly complex, so does the complexity of protecting sensitive data from deliberate or accidental exposure. As a result, more organizations are concerned with where their sensitive data is, who has access to it, and how they can reduce the risk of the data being compromised.

Data Loss Prevention (DLP) and Identity and Access Management (IAM) technologies are both all about reducing risk.

DLP products discover, monitor, and protect confidential data wherever it is stored or used. DLP answers three fundamental questions:

- Where is your confidential data?
- How is it being used?
- How do you prevent data loss?

IAM, on the other hand, tackles:

- Who has access to the confidential data across your organization?
- What can they do with the confidential data?
- Which users represent the greatest risk based on who they are and what they can access?

IAM and DLP Synergy

Until recently, DLP and IAM solutions worked separately, and IT and security managers were unable to leverage their complementary capabilities in a unified solution.

Today, Courion is addressing this problem by delivering Sensitive Data Manager, a solution that integrates ComplianceCourier[™]—Courion's access compliance and identity management solution—with leading DLP vendors, such as Symantec, RSA, and others, that enables your organization to answer the questions:

- *Where* is my confidential data?
- *Who* has access to it?
- *How* did they obtain access?
- *What* are the risks associated with that access?
- *How* should I reduce these risks?

When a DLP scan discovers sensitive data, it evaluates if the data is vulnerable to external exposure, alerts the appropriate personnel and takes steps to protect the data. However, in many instances the data owner or security manager will want to know who has access to this data, how they gained the access, and what impact it has on the risk that the data may be compromised.

Combining DLP and IAM makes it possible for managers to make more intelligent decisions concerning the appropriate response to a DLP alert, by enabling them to more easily determine the level of risk associated with a specific alert. They can do this by identifying which users have access to the sensitive data and evaluating whether their access rights are appropriate or not.

Combining IAM with DLP provides managers with detailed identity-based context for the DLP alert, such as: name, title, department, manager, location, entitlement, group memberships, etc. This additional context enables the manager to evaluate the level of risk associated with this access. For example, when DLP discovers customer credit card data on a SharePoint site, the combined solution can highlight that “Joe” in Accounts Receivable has access, which is appropriate, along with “Fred” in Engineering, which is not appropriate.

Sensitive Data Manager takes the next step by allowing the manager to implement the most appropriate remediation strategy, based not only on what kind of data has been found, but who has access to it. These steps may include:

- Approving the user access rights and documenting the reasons why
- Modifying the alert level
- Creating an email message or help desk trouble ticket
- Notifying the DLP solution to encrypt the data or move it to a more secure location
- Modifying user access rights
- Blocking access for individual users or specific groups of users.

Integrated Solution

Sensitive Data Manager is part of ComplianceCourier—Courion’s access compliance solution. ComplianceCourier automatically manages the access compliance and certification process by notifying authorized managers when it is time to review employee access rights and activities, and enabling them to confirm that the employee’s access complies with corporate policy or relevant industry/government regulations (SOX, PCI DSS, HIPAA, GLBA, etc.).

If access rights to enterprise resources need to be changed, ComplianceCourier can automatically trigger the appropriate actions to initiate corrections, using a variety of remediation options. An audit trail tracks all review and remediation transactions undertaken by authorized managers.

Access Certification and Compliance Management Features

Compliance and Attestation	Effectively respond to auditor and regulator demands for data demonstrating compliance with corporate policies or key industry and government regulations.
Automatic Notification	Automatically notify or periodically remind business managers when it is time to confirm user access rights according to company policy.
Designed for Business Users	Provide security and business managers with a business-friendly view of entitlements to confirm or remediate user access rights.
Comprehensive Data Integration	Identify users with access to sensitive data (DLP) or review prior activity (SIEM) to ensure compliance with security guidelines. Identify and remediate segregation of duties violations.
Integrated Remediation	Automatically initiate corrective actions, without the need to install a provisioning solution.
Audit Tracking	Track and store transactions for audit tracking or forensics analysis.

For more information on the benefits of integrated DLP and IAM, contact Courion at info@courion.com.

