SPIRION

SOLUTION OVERVIEW

Invoking advanced rights management with accurate identification

Making sure valuable data remains secure while allowing it to be shared across networks, cloud applications, and devices is a challenge that cannot be solved with a single tool. The volume, variety and velocity involved demands a best-of-breed combination that is focused on locating and identifying the most valuable and most vulnerable assets while delivering file-level protection that keeps organizations in control of their assets both within and outside of the enterprise.

The most accurate data identification delivers the most accurate protection

Data can't be properly protected if its sensitivity isn't completely understood. Spirion data identification solutions help discover, classify, and remediate sensitive data wherever it lives, with industry-leading accuracy you can trust. Spirion helps organizations understand the information hidden in the data they hold so appropriate controls can be applied.

Spirion performs fast and accurate searches of both structured and unstructured data in ways that even seasoned end-users cannot; including data mining within images, on hosted and on-premise email servers, databases, employee laptops, SharePoint and the cloud. By leveraging the automation and accuracy of Spirion sensitive data identification, organizations can more accurately focus their data security spend and protect sensitive data.

Seclore delivers fine-tuned control over data protection

With the datacentric security platform from Seclore, you have options that go beyond mere encryption. Once files are protected with Seclore, the information stays protected with granular usage controls wherever it goes—inside or outside the organization.

SECLORE

Seclore Rights Management can apply various levels of control to ensure data is protected regardless of how it travels or where it is located. Files protected by Seclore offer detailed and specific control over data handling that include:

- **Who can access the data**
  - Specific internal or external users and groups
- **What individuals can do with the data**
  - View, edit, print, cut-n-paste, screen capture, etc.
- **When individuals can access the data**
  - Grant or revoke rights on a time-specific basis, e.g. time-bombing
- **Where individuals can access the data**
  - Location-based controls can restrict which devices or geo-locations the rights apply

How Spirion and Seclore are better together

Discovery tools do a great job of discovering and classifying data while providing customers with tools to effectively monitor it. The problem, in many cases, is that the data in question may have already left the enterprise, placing organizations in a chasing game – chasing their data, and chasing their "bad actors."

Rights Management solutions have shown to be an effective way to protect data no matter where it lives, but can sometimes rely too heavily on untrained users to determine when to apply policies, and which policies should be applied to each and every document. Additionally, Rights Management solutions are able to provide precise policies and controls only when the data has been accurately identified.

The Seclore-Spirion integration represents a unique combination of privacy-grade identification tools and file-level security. Organizations deploying this combination gain the ability to better understand the sensitive data they possess while securing it wherever it travels. Deploying this best-of-breed approach will significantly improve organizational security against data breaches and compliance violations.

How it works

Based on detected sensitivity, Spirion industry-leading discovery and classification can be configured to automatically invoke Seclore's data-centric security controls such that information is always protected. The protected data is now completely auditable, whether it resides inside or outside the safe confines of the enterprise. This combination means the customer is no longer required to chase their data; Instead gaining invaluable insights as to how their data is being used instead of abused. Access to the data, including the complete revocation of access, may be modified at any point in time, further protecting organizational interests while adhering to regulatory compliance.

01 user creates a file

02 ...and saves into a folder

03 Spirion scans file for metadata, keywords and patterns

04 On policy violation, file gets protected with Seclore

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion has relentlessly solved real data protection problems since 2006 with accurate, contextual discovery of structured and unstructured data; purposeful classification; automated real-time risk remediation; and powerful analytics and dashboards to give organizations greater visibility into their most at-risk data and assets. Visit us at spirion.com