Using Data Loss Prevention for Financial Institutions

Banks, Credit Unions, Payments

How Data Loss Prevention (DLP) Technology can Protect Sensitive Company & Customer Information and Meet Compliance Requirements, PCI- DSS

Disclaimer: This white paper is not intended to provide legal guidance for PCI-DSS, GLBA, SOX compliance. If you have questions about the meaning of particular provisions of these regulations, you should consult your attorney.

The Somansa® Data Loss Prevention product suite is a tool that people can use to help them comply with these requirements,

SOMANSA

SOMANSA Data Loss Prevention (DLP) Introduction for Financial Institutions

Financial service institutions worldwide chose Somansa to protect sensitive data and meet compliance requirements

Somansa Data Loss Prevention solutions provide financial service institutions, banks/credit unions, investment firms, and credit card and payment companies the most comprehensive security solution to protect sensitive company and customer data including credit card and social security numbers while helping meet regulatory compliance requirements.

> ***"The average cost of a corporate data breach increased 15 percent in the last year to $3.5 million."***
> ***Ponemon Study, 2014***

Somansa provides a complete Data Loss Prevention (DLP) solution to Discover, Monitor, and Protect Sensitive Data

- **Monitor and Prevent** sensitive company and customer data leakage through Network Protocols, Email, Webmail, FTP, Network Share and Removable Storage, USB, iPads, Printing, and Databases.

- **Discover** by scanning and locating sensitive data on endpoints, laptops, PCs, and servers based on pre-defined and customizable detection methods and polices.

> ***"20 million customer's data stolen from 3 credit card companies using USB devi ce. "***
>
> ***New York Times, 2014***

Meet Regulatory Compliance and Audit requirements related to financial service institutions with Somansa

- **Comply** with PCI DSS, HIPAA, Sarbanes-Oxley (SOX), GLB, etc.

CONTENTS

Main PCI-DSS requirements

Requirement 3: Protect Stored Data
Requirement 7: Restrict access to cardholder data by business need to know
Requirement 10: Track and monitor all access to network resources and cardholder data

- Identify sensitive company and customer data
- Where is the data located
- How is data used

PCI DSS (version 2.0), mandates DLP data discovery functionality by stating that a merchant should "confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data.

Enforce controls to protect the data.

1) Define PCI DSS policies
2) Remediation
3) Enforcement- after identifying policies and data location, enforce data protection
4) Reports

Using Somansa DLP

Data Discovery:

- Run on storage and endpoints
    - Customer data including credit card and account numbers
    - Scan for inappropriately stored credit card and sensitive data on laptops, desktops, and servers

Remediation:

- Enforce policies to protect data

Data Protection and Compliance with Somansa Data Security

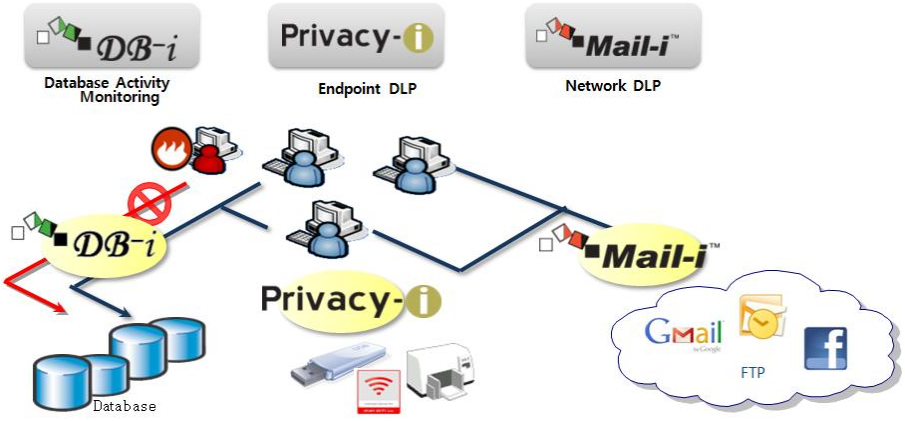
As more corporate data and confidential information is being exchanged through the network via Email, IM, FTP, Databases, and stored/transferred to USB's and portable storage devices, the liabilities and amount of resources exhausted for financial institutions have also increased. Confidential and sensitive information leakage, meeting compliance regulations, penalties and legal lawsuits, and brand damage can all lead to financial and resource loss for organizations.

Data loss, whether intentional or unintentional need to be addressed.

- Employee uses personal webmail (ie. Gmail, Yahoo) to send sensitive customer data from home to work
- Employee copies customers' credit card numbers to USB/removable storage
- Posting confidential company information to social networking (ie. Facebook, Twitter)

Somansa is an affordable and easy to use data security solution designed for organizations to meet regulatory compliance in the financial services industry such as PCI-DSS while protecting sensitive company and customer data. Somansa provides financial institutions with a complete data security solution that includes network and endpoint DLP features to Monitor, Protect, and Discover confidential and customer data.

HOW IT WORKS

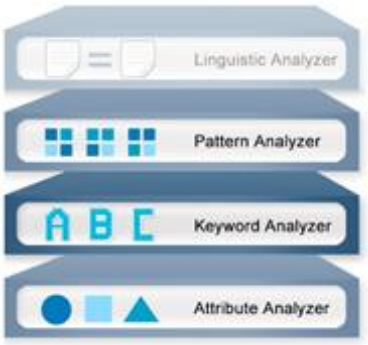


Somansa Monitors, Discovers, and Prevents sensitive data in the company network

SOMANSA

POLICY SETTINGS

Based on defined policy rules, Somansa DLP monitors and detects sensitive company and customer data in motion (Network) or at rest (Endpoint). Policies can be defined according to Users/Departments, IP Addresses, Protocols, Keywords- Patterns related to specific industries or Compliance including:



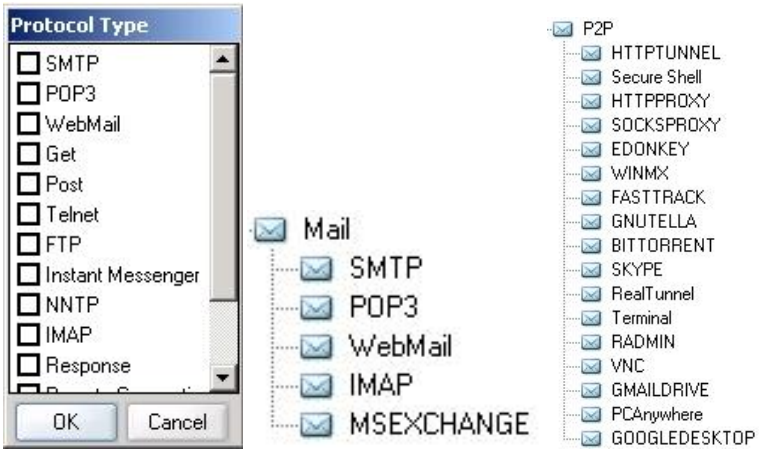
Data Monitoring

- Social Security Numbers
- Credit Card Numbers
- Medical Record Numbers
- ABA Bank Routing Numbers
- Document Matching (Hash)

Monitor and Prevent Data Leakage through Network Protocols, Email, Webmail, FTP, Network Share and Removable Storage, USB, iPods, Printing, and Databases.

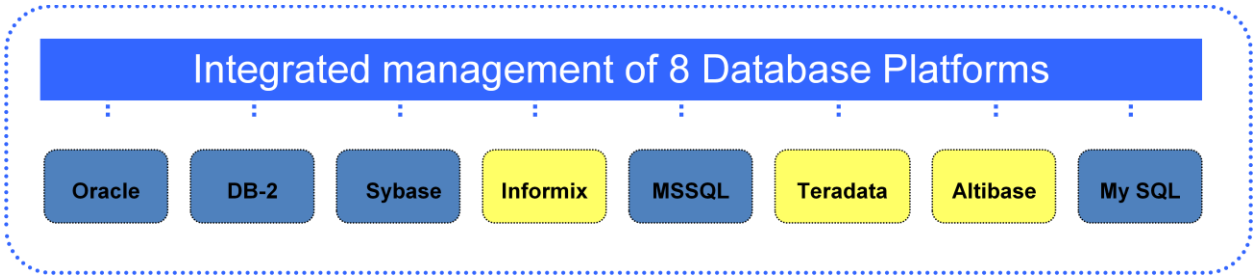
Discover sensitive data on endpoints by scanning and locating data on desktops, laptops, servers based on pre-defined and customizable detection methods and polices.

NETWORK PROTOCOLS



Somansa supports more messaging protocols than any other DLP product.

DATABASE AUDIT & PROTECTION (DAP)

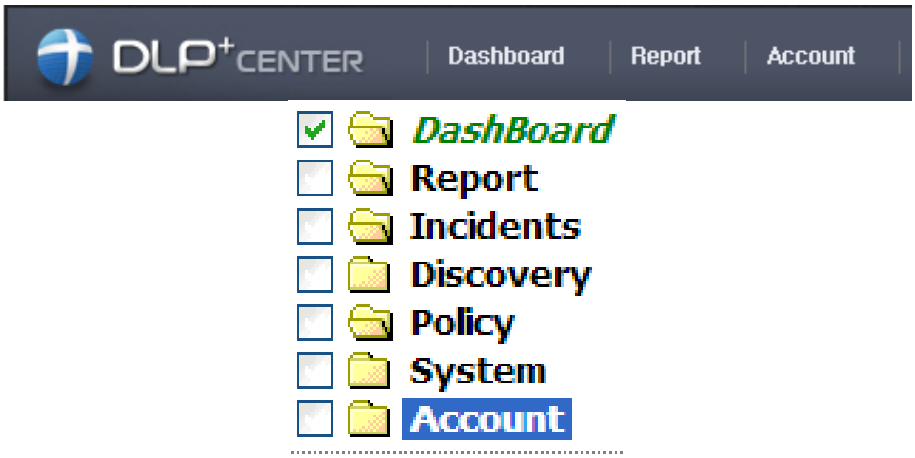


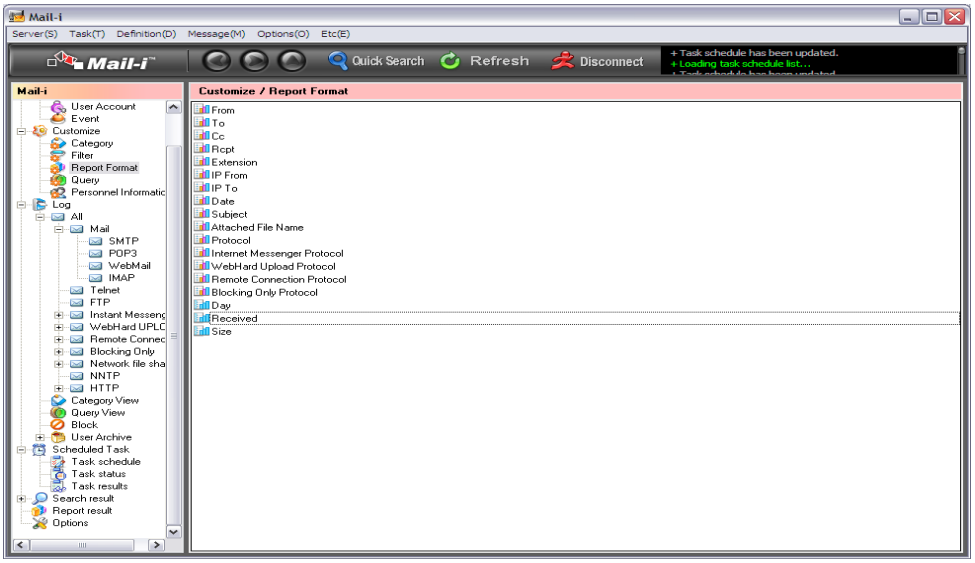
- **Central Management:** Supports various database platforms.
  - Mirroring, In-line, or Proxy methods to monitor data.

- **Monitor and Record:** Monitor data from all access points to the database including Console Access, AP Server, and Query Tools.

- **Security:** Access and Change Control ID and Password validation, Policy Settings, User Audit, and Real-time Alerts and Reports.
  - Plus, Data Masking (ie. credit card numbers)

DASHBOARD-REPORTING





Somansa provides status user/event reports including audit trails.

Compliance Requirements	Somansa DLP Solution
PCI-DSS	
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for businesses, legal, and regulatory purposes, as documented in the data retention policy	Using Somansa Endpoint DLP functions to Monitor and Discover cardholder data stored on desktops, laptops, and servers that are in violation of the PCI data retention and disposal policy.
3.2 Do not store sensitive authentication data subsequent to authorization. Sensitive authentication data includes the data as cited in the requirements 3.2.1 to 3.2.3	Discover sensitive authentication data and take action using Somansa Endpoint DLP policy rules.
3.3 Mask the primary account number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed)	Credit card numbers and other sensitive data can be masked using Somansa Database Audit & Protection solution based on user access through the policy rules function.
7.1 Limit access to system components and cardholder data ton only those individuals whose job requires such access.	Identify cardholder data stored in desktops, laptops, servers, and databases and enforce user rights to access the data with Somansa Endpoint DLP and Database policy rules.
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Restrict file access to specified users based on the type of information and enforce user rights to access the data with Somansa Endpoint DLP and Database policy rules.
10 Track and monitor all access to network resources and cardholder data.	Based on policies rules, cardholder data including credit card numbers viewed or transferred via email, copied, FTP, print, etc. can be monitored with Somansa Network, Endpoint DLP and Database functions. Alerts and Reports are also provided for audits.

SOMANSA Data Loss Prevention (DLP) Introduction for Financial Institutions

"After evaluating several other solutions, Center Bank selected Somansa to identify and protect confidential company and customer information. "The majority of our customer and confidential company information is stored in electronic format," said Jae Choi, Director of IT for Center Bank. "We needed a solution that would protect our data and meet compliance and regulatory rules."

About Somansa

Somansa is a global leader in Data Security and Compliance solutions designed to protect valuable company information from leakage and help meet regulatory compliance requirements.

Using its advanced packet and protocol analysis technology, Somansa provides a total security solution to Monitor, Protect, and Discover sensitive company data in motion and at rest including network protocols, email, IM, FTP, endpoints such as USB and Database activity to meet regulatory compliance requirements while protecting valuable company information.

www.somansatech.com

For more information please contact:

Tel: (408) 701-1302 Email: sales@somansatech.com

SOMANSA