



Information Security (PII)

www.chiliad.com

Solution Overview

"...Incidents compromising personally identifiable information (PII) are occurring at an alarmingly high rate, with more than 85% of survey respondents reporting some type of reportable privacy breach..."

In today's global economy with its global enterprises, transparent borders, and technological advances, vast amounts of data - private data - migrate across states, countries and continents instantaneously. Organizations too are becoming more complex with a wide web of customers, partners, and vendors, who have access to personally identifiable information (PII). Protecting this data from identity theft is paramount.

PII is any piece of information which can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In 2008 alone, there were 638 breaches with 34.1 million records affected. Public concern and regulations to protect PII are mounting. Adhering to these regulatory requirements and protecting PII is now an even bigger challenge. Information on citizens including Social Security Numbers (SSN), names, addresses and credit card data traverse the globe, every second. For an organization to minimize inadvertent loss, limit exposure, and prevent malicious attacks they need to effectively manage the governance, risk and controls of their PII. Identifying every nook and cranny that stores any form of PII is the most critical step to accomplishing this.

"...By having an up-to-date view of where PII exist ...you can effectively review your policies and processes, and take corrective action as appropriate to ensure your institution has adequate safeguards..."

Fast, Efficient, Accurate, Laser Focused, Searches

Information Security Officers, Risk Managers and Security Analysts all have the same fundamental business drivers, questions and challenges - protect private data.

- They are driven to improve the organization's ability to efficiently govern, control and protect PII data while managing labor resources.
- They need to know, identify and access PII data from all available sources to enable proper audits, security controls and management of this data.
- They are challenged to minimize the time and cost associated with identifying and auditing this data.

Organizations and information security workers need Chiliad Discovery/Alert. With Chiliad Discovery/Alert you identify all your PII data irrespective of location. By having an up-to-date view of where PII exists in your organization you can effectively review your policies and processes, and take corrective action as appropriate to ensure your institution has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.

Features Include:

- Support for globally distributed data as well as data in legacy systems
- Support for unstructured and structured data
- Global ranking of results across all distributed data
- Single access point for all authorized data
- Data batching capabilities
- Federated search capabilities
- Contextual searches
- Search logging and tracking capabilities
- Faceted navigation for searches
- Real-time filtering and search alerts
- Integration with external data
- Support for multi-user data searches
- Distributed environment with nodes
- Geospatial options displays data such as entities and search results on a map

Benefits

Chiliad Discovery/Alert advantages include:

Streamlined Audit Processes: Simplify and extend the audit process with automated data interrogation of disparate data sources (both structured and unstructured). Through Chiliad's built-in concept recognizer and extraction capabilities, you can quickly perform a complete audit of all your data for any PII. This also eliminates error prone, time consuming, repetitive, and ineffective PII searches, increases accuracy and empowers employees who can now redirect energies to other projects.

Accelerated Audit Cycle: Enable quick action on any new PII with sophisticated real-time monitoring and alerts. This allows you to know immediately when any new PII data is stored so the audit team can ensure that data is properly assessed and the needed controls employed.

Minimized Risk: Manual PII audits are difficult. All the various disparate data sources are typically large, thus only a subset can be audited for PI. This exposes the institution to the risk of unintentional or malicious security breaches. Chiliad's speed minimizes the risk of this occurring.

Accurate Reports: Chiliad allows you to create reports and thus a trail and history of your PII data. This quickly educates new data security specialist on PII locations. It is also an excellent tool to dictate where PII policies and procedures are needed and can be used to demonstrate compliance.

Categorization of PII Result: Chiliad allows you to categorize PII data so that you can then institute the needed controls and enforce security and privacy policies.

Quick Return on Investment (ROI): Reduce the costs of regulatory audits by lessening the manpower and time associated with finding PII across your enterprise. PII searches typically require an intensive, manual process by which data sources such as file shares, websites, and databases are reviewed by information security personnel.

Chiliad Discovery/Alert solves stovepipe issues and promotes quick PII audits:

- Does not disrupt existing systems
- Allows individual departments, divisions, business units, agencies and organizations to maintain control and management oversight over their information
- Does not place excessive burden on network bandwidth and computing resources
- Is scalable in terms of data volume, number of data sources, number of users and network distribution
- Provides the most relevant results, and a rich, navigatable knowledge base for analysis and drill down regardless of how diverse and large the target data repositories