MinerEye Solutions

for Information Governance and Data Privacy Compliance

minereye

www.minereye.com

minereye

Solutions for:

Data Discovery & Governance

1. Data mapping for dark and unstructured data
2. Automated risk quantification of personal information (PI) and sensitive business information.

Data Privacy Compliance

1. Privacy regulations compliance for every file (GDPR/CCPA/PIPEDA/ LGPD/CMMC, etc.)
2. D/SAR compliance with the right of deletion and FOIA requests for personal information & rectification regulations
3. Compliance with data minimization regulations

Cloud Data Optimization

1. Smart cloud migration
2. Data retention

Data Protection & Secure Collaboration

1. Data protection in file sharing – Granular classification and policy enforcement
2. Data protection policy modeling with virtual multiple labeling

Incident Response & Breach Notification

1. Compromised PI and business information data one-time reporting
2. Continuous PI and business Information risk assessment

Data Discovery & Governance

Challenges

Organizations have zero visibility into what lies within their unstructured data making correlation between file data and a specific requirement practically impossible (e.g. privacy, business, security policies, geographic regulations).

Organizations suffer from an inability to manage the huge data volume without the tools to identify risk within that data and to prioritize the handling of the risk.

MinerEye Solutions

- Data mapping for dark and unstructured data
- Automated risk quantification of personal information (PI) and sensitive business information

Solution description

Provides automated visual mapping so that file data can be analyzed easily for multiple dimensions. For example, multi-national organizations need to map data according to geographic security, privacy regulations and business policy interests.

Automated continuous assignment of a risk score per file by analyzing the variety and quantity of PI entities and sensitive business information contained in a file.

Technology description

Leverages AI and ML to scale down the big data challenge and groups information about file data in a variety of dimensions (e.g. meta-data, content, risk, location, permissions).

Puts a risk score to every cluster or classification for clear-cut prioritization.

MinerEye Advantages

- Provides multi-dimensional mapping within seconds.
- Automates applying risk scores in a unified view across file types and data sources giving end users the flexibility to customize.

Data Privacy Compliance

Challenges

Extraordinary time and resources are required to comply with each compliance article on the file level.

In certain geographies, consumers have the right to request information about how their personal data is used and request that the data is deleted. Finding their data is typically performed manually in a long and expensive process. If not completed within the prescribed time, delays come with penalties.

GDPR requires data minimization, only retaining personal information (PI) for purposeful processing. Finding PI information in unstructured data is a long and time-consuming process.

MinerEye Solutions

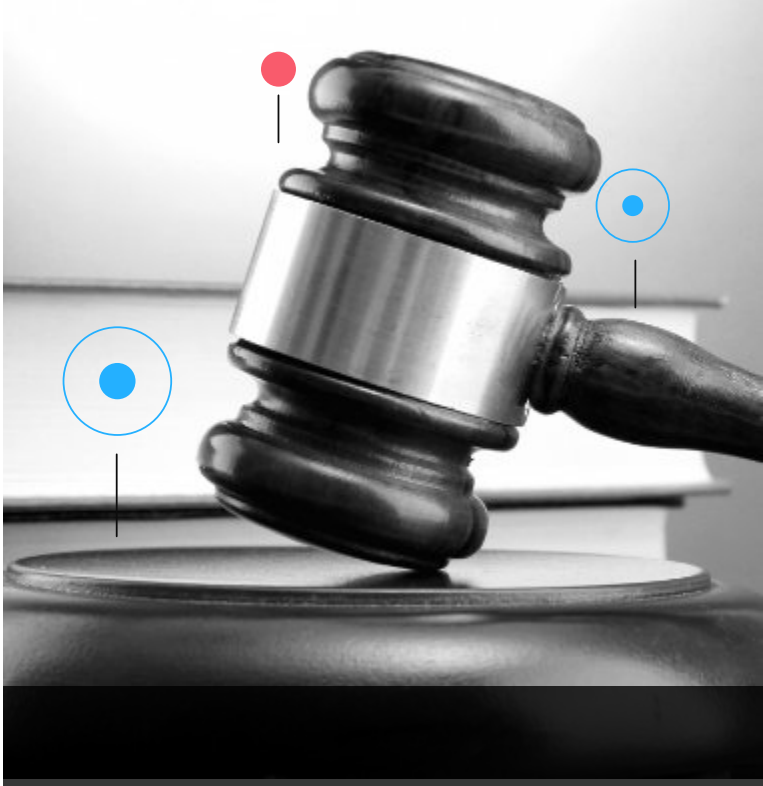
- GDPR/CCPA/PIPEDA/LGPD/CMMC/ etc. regulations compliance
- D/SAR and FOIA compliance (requests for deletion, for personal files, rectification)
- Data minimization

Solution description

Aggregates information about the data in the context of articles within the privacy compliance regulations.

Automates finding and continuously tracks a person's data within seconds so request can be fulfilled.

Automates the discovery of PI data in files and maps them according to the prescribed use as per each GDPR article. Continuously updates compliance and alerts those files containing non-compliant data.



Technology description

Maps the file data to logical and geographic data residency issues.

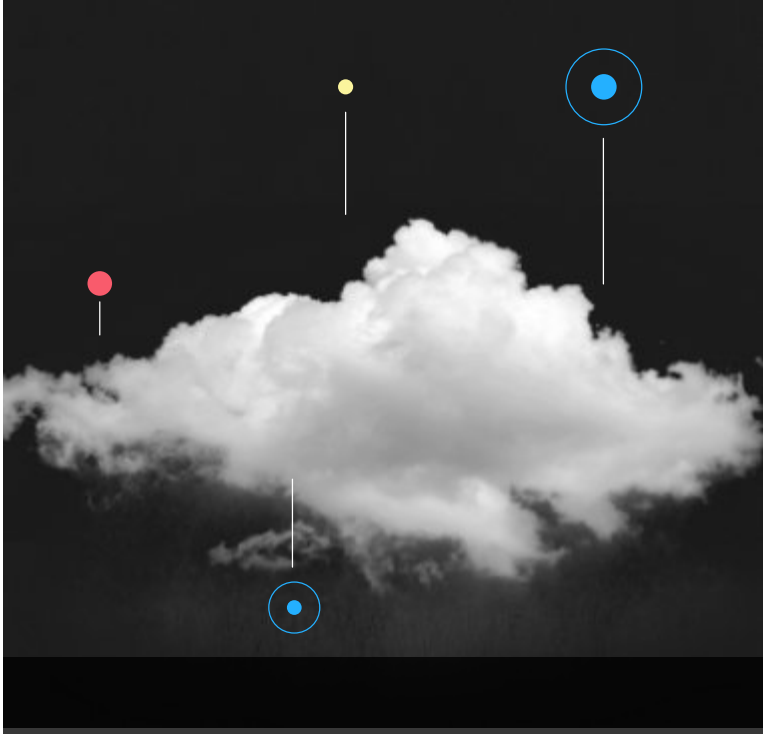
Automatically indexes PI data (personal information) and stores it as searchable entities.

Categorizes the file data based on advanced analysis of context and content to help the user understand the purpose and use of the file data.

MinerEye Advantages

- Contextual and continuous monitoring of privacy compliance on the file level of unstructured data.
- Comprehensively searches among multiple sources and formats of data within seconds.
- Automatically analyzes the context of file data which implies the way the data is being used. The only solution that collects and clusters multi-dimensional file data from multiple types and sources, including both cloud and on-prem.

Cloud Data Optimization



Challenges

Adopting cloud infrastructure can be extremely costly if an organization's data is not scanned and cleaned of redundant, obsolete and trivial (ROT) files.

In a hybrid environment of multiple cloud use, organizations experience data sprawl that makes the application of data retention policies exceptionally challenging and at times impossible.

MinerEye Solutions

- Smart cloud migration
- Data retention

Solution description

Automated and continual analysis and categorization of data that identifies ROT file data that should not be moved to the cloud.

Normalizes the data via visual analysis, across the hybrid cloud environment. Continuously supports and monitors the implementation of data retention policies that significantly reduces cloud costs.

Technology description

De-duplicates and identifies near duplication using visual correlation of file data.

Leverages cloud APIs to continuously analyze the data on a granular level and how its categorized for optimal data retention.

MinerEye Advantages

- Efficient automation on top of big data analyzes a variety of formats and platforms finding both the actual duplication and the "near duplication" data minimizing migration costs from 30-50%.
- Correlating multiple dimensional analysis that enables granular dissection of data, thereby enabling implementing customized data retention policies.
- Automated, fast identification of duplicate files in unstructured data including attachments, teams messaging and graphic objects, OCR/ Images, scanned PDFs, Office, text/csv and binary data.

Data Protection & Secure Collaboration

Challenges

The massive increase of cloud platforms in a hybrid environment has resulted in an uncontrolled file sharing of business critical and sensitive data across all internal business units and as well as externally.

The many mistakes and false positives in legacy file labeling and policy enforcement tools cause organizations to either abandon the process completely or to misclassify files. In both cases, organizations are vulnerable and their shared files will eventually be mishandled.

MinerEye Solutions

- Granular classification and policy enforcement of shared files
- Data protection policy modeling with virtual labeling & integration with Microsoft365 and encryption

Solution description

Automated identification and labeling of business critical and sensitive data to enable secure and compliant cloud collaboration, access control, rights management and encryption across a hybrid environment.

Enables policy simulation and fine tuning of the desired result before invoking the policy action. This optimizes the accuracy and reduces false positives, improves the protection and reduces the overhead of security teams. Enables true policy enforcement with protected file sharing.

Technology description

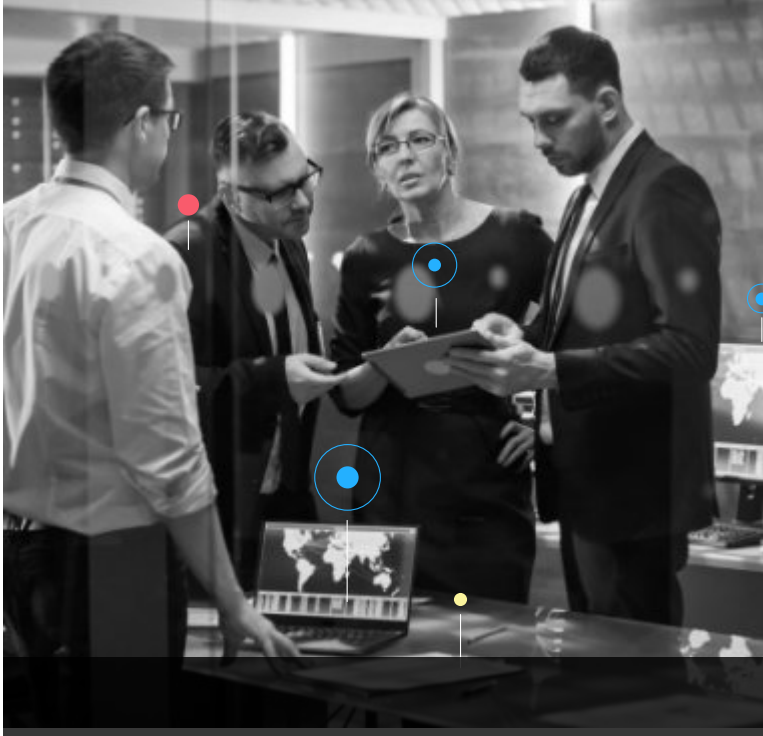
Automates classification using multi-dimensional machine learning analysis that enables virtual labels.

Centralizes, continuously indexes and models the data, allowing for virtual policy simulation, particularly valuable when policies of security, privacy and business operations may be in conflict.

MinerEye Advantages

- Enables the granularity of multiple labels to relate a single file to multiple virtual labels. This enables organizations to use detailed granular data protection policies, according to file content, context and user.
- Performs classification in an isolated manner from the policy implementation, thereby enabling the synchronizing of an organization's operational, security and privacy policies with continual updates for granularly accurate policies for protected file sharing.

Incident Response & Breach Notification



Challenges

Reporting the results of a breach to regulators and the compromised individuals within a specified timeframe is done manually, taking months and never discovers all the compromised data. In addition to reporting due to regulations, data breaches cause brand damage and customer attrition. However, detailed and fast data discovery before the breach is publicized can mitigate these negative effects.

Organizations have no visibility into its dark data making data protection an impossibility and leaves data exposed to leakage. As regulatory bodies from all directions are mandating reporting and granular data handling, organizations are very challenged to do so in its unstructured data.

MinerEye Solutions

- Compromised PI and business information data one-time reporting
- Continuous PI and business information risk assessment

Solution description

Fast and detailed breach notification discovery within unstructured data down to the PI and business information entity detail in seconds.

Identification of similar files within unstructured data to the ones breached, where they are stored and who has access.

Technology description

Proprietary AI technology used to scan and import terabytes of data.

Intelligent data risk assessment with risk scoring and prioritization of risk.

Maps and detects PI and business data entities within compromised file data and categorizes it in any manner required.

MinerEye Advantages

- Fast deployment for automated discovery with accurate results in a matter of hours to alert data compromise for immediate mitigation of breach incidents.
- Automated, fast discovery of sensitive information down to the PI and business information entity detail in unstructured data including attached files, teams messaging and graphic objects, OCR/Images, scanned PDFs, Office, text/csv and binary data.

Who we are

MinerEye has developed a disruptive, award winning AI technology that tracks sensitive personal and business data in an organization's unstructured data repository.

MinerEye has reimagined sensitive data security by offering a completely new way to look at unstructured data and identify it by its detailed entities. Employing computer vision to illuminate the masses of "dark data" that exist in organizational data repositories and in the cloud, MinerEye illuminates areas that would otherwise remain dark and invisible.

MinerEye enables organizations to overcome the information governance, privacy and protection challenges. Its Interpretive AI™, machine learning and computer vision automatically scans, analyzes, virtually labels and indexes and categorizes unstructured and dark data contained in organizations' data repositories. MinerEye's customers may be found across financial, IT, manufacturing and other verticals worldwide.

REQUEST A DEMO

www.minereye.com
info@minereye.com