MinerEye Solutions

Incident Response & Breach Notification

www.minereye.com

minereye
See Beyond Data

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 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

Incident Response & Breach Notification of Compromised Unstructured Data

Problem

Following a cyberattack or data exfiltration, data analysts and risk management consultants typically spend from weeks to months manually scanning user email accounts that may have been compromised. This painstaking task of reviewing inboxes and emails one-by-one can often lead to mistakes, in addition to its high cost. Once the compromised files and emails are retrieved, a second process is required to identify what entities of information were leaked, as well as the level of potential harm to the data owner by the breach. Finally, a breach often requires a third process to categorize compromised user data according to the risk of potential fraud and malicious use, such as posting the data for sale on the dark web.

Fast action minimizes damage. When a breach occurs, tensions run high in the company at the thought that its crown jewels – its assets, its reputation and possible customer attrition – are at risk. Aside from business considerations, the regulatory responsibility of reporting within a specific time frame comes with heavy fines. Yet, at the moment of a breach discovery, most organizations are forced to hire qualified experts and mobilize their internal IT staff to locate the documents, emails and files on local and cloud servers that contain personal information (PI) and sensitive business information. The problem with this manual method is its typical timeframe of weeks, or even months delivering cursory and incomplete results.

Discover Compromised Data in Minutes

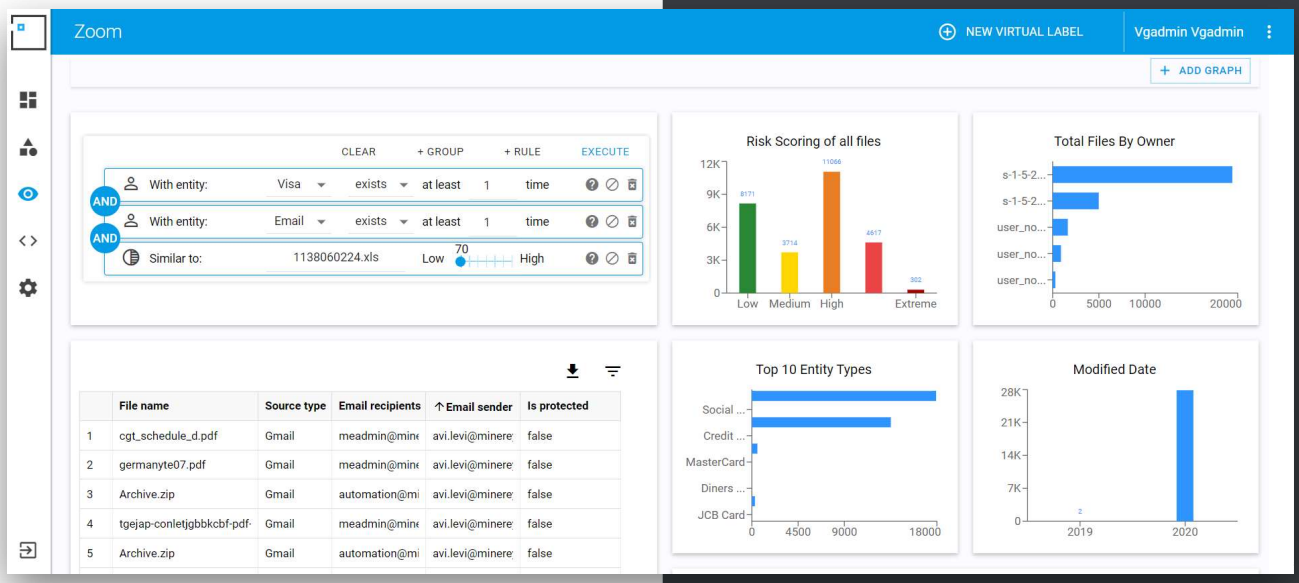
Breach Notification Challenges Solved

- Fulfill regulatory compliance (e.g. CCPA, GDPR, PIPEDA, NYPA, FOIA, LGPD, GLBA, CMMC) that mandates specific timeframes for reporting and the detailed content of the compromised data
- Typical manual discovery methodology is very expensive and takes weeks, sometimes months, leading to punitive fines
- Results often miss data entities that are hidden in a hybrid environment of cloud and on-premise systems
- Unstructured data is not picked up by most automated scans

"Beyond shaving weeks off of a typical manual scan, by using MinerEye we were able to uncover data files that were randomly labeled and contained thousands of sensitive personal information (PI) within minutes"

"This confirmed that the combination of MinerEye's AI-based data discovery solutions and our professional cyber services is clearly the fastest and most effective approach in addressing incident response"

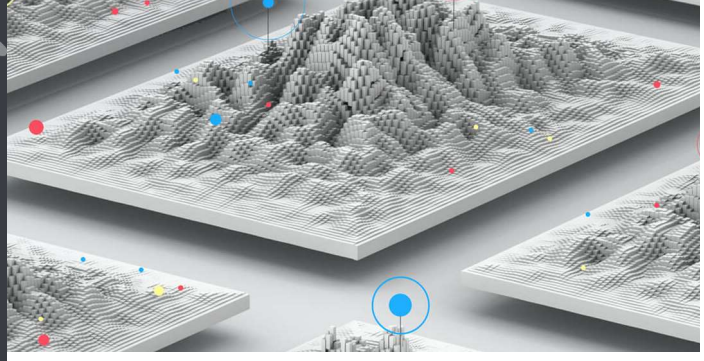
Will Xiang, Vice President
Cyber and Privacy, RICHTER.



MinerEye's Post Breach Compromised Data Reporting

With MinerEye's solution for Compromised PI and Sensitive Business Data Reporting, MSSPs can automatically discover and monitor customer data, on premise or in the cloud. This AI-driven platform can easily find sensitive unstructured data throughout a hybrid environment by auto-learning from sample documents, map data locations and chart data owners' information. Within seconds, MSSPs pick up information from unstructured data including attachments in emails, teams messaging, and graphic objects, OCR/Images, scanned PDFs, Office, text/csv, and binary data.

Way beyond basic data discovery, MinerEye tells the story of the data in question, amplifying a managed security services provider's (MSSP) incident response and investigation services. MinerEye enables a service provider to prescribe a risk score per file, explaining how the compromised data was used, in what files, by which user accounts and across which systems.



Compromised Account Review for Breach Notification

- Tell the story of how your customers' compromised data was used, identify files in which the compromised data was located, by which user accounts and across which systems
- Define and discover data context and zoom into details of the data entities
- Achieve multi-dimensional mapping in seconds: By size, extension, AIP label, detailed entity level, user information and who had data access
- Show segment geo-location by server location
- Intelligent data risk assessment with risk scoring and prioritization of risk
- Identification of similar files to the ones breached, where they are stored and who has access
- Use intelligent data forensics to neutralize threats
- Know what data is at-risk, sensitive or regulated
- Remove, quarantine, or archive critical data

Customized for MSSPs Ease-of-Use

- Private secure cloud configured per client
- Rapid deployment and time-to-operation
- Proprietary AI technology used to scan and import terabytes of data
- Flexible pricing model with various data packages per month, or per mailbox accounts, all of which may be scaled up on demand

Propel the Productivity of your Managed Security Services

Leveraging computer vision and machine learning technologies, MinerEye illuminates masses of "dark data" that exist in organizational data repositories and in the cloud. MinerEye discovers, protects and tracks not only unsecured corporate data and sensitive customer data, but also all of the locations and duplicates and near-duplicates of sensitive documents for minimized risk and easy compliance to audit requests.

MSSP Benefits by Integrating MinerEye in its Service Portfolio

- Increase revenues with higher margins in your incident response and breach notification services
- Automate the discovery, reporting and ranking process of a breach
- Increase productivity – cover more customers with the same team
- Significantly cut costs with more accurate, comprehensive results
- Stay on schedule for regulatory reporting
- Reduce the need for expertise personnel

Who we are

MinerEye has developed a disruptive, award winning AI technology that tracks sensitive data wherever it resides and whatever form it takes.

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