minereye

HOW MINEREYE SUPPORTS MSSPS' UNSTRUCTURED DATA PROTECTION AND PRIVACY COMPLIANCE SERVICES

Flexibility and Speed for Maximum Value

Many Managed Security Services Providers (MSSPs) are feeling the pain of their customers' reductions in their cyber defense investment due to the economic difficulties of the pandemic. Yet, many of these same enterprises invested significantly in collaborative software to facilitate "working-from-home". This chasm has caused a gap in organizations' readiness to protect their data from cyber threats and data leakage on their very extended attack surfaces and increased ease of file sharing.

Simultaneously, data privacy regulators have not let up on their enforcement of customer data protection compliance. Market analysts such as Gartner cite that more than 80% of enterprise's data fall in the category of unstructured (or dark) data. This means that customer private information (PI) and sensitive business data are primarily located within the email attachments, archived files of employees, local shared folders and in cloud-based storage drives. This data is typically accessed only by manual means, and with the voluminous data sprawl of many cloud-based repositories, it's nearly impossible to map and protect this sensitive and regulated data with speed and accuracy. Without access, privacy compliance and data protection are unfeasible.

Access & Governance of Unstructured Data Solved by MinerEye

MinerEye enables MSSPs to provide customers with the many efficiencies offered by the cloud while still fully protecting their data from hijacks or disclosure. MinerEye offers MSSPs the ability to demonstrate to customers how they protect data, maintain PI privacy, ensure data residency compliance, and keep updated on the regulatory environment.

1 Data Discovery & Mapping of Unstructured Data

MSSPs can offer a light assessment via a quick scan of an organization's data health and find those files in high risk of breach or non-compliance of a specific regulation. A customer's unstructured data repository can be visually mapped in minutes analyzing the data in multiple dimensions, such as geography, data entities, privacy regulations or business policies.

3 Incident Response and Breach Disclosure for Notification

Following a breach, MSSPs can discover potentially compromised data, both PI and sensitive business data within the organizations' emails and file repositories within minutes. With MinerEye's quick and accurate scans of unstructured data repositories, on-premise or in the cloud, MSSPs can comply with regulatory breach notification, while mitigating brand damage and customer attrition.

2 Cloud Data Optimization

Most enterprises are moving towards a hybrid cloud strategy, using numerous SaaS technologies harboring endless pieces of personal and business sensitive data. Given the massive risk in migrating huge volumes of files to the cloud with no way of accessing this sensitive data, MinerEye can enable MSSPs to protect and minimize this sensitive data. By extracting the data to a simulated modeling environment, MinerEye syncs an organization's security, privacy and business operational processes to classify each file with multiple, virtual labels.

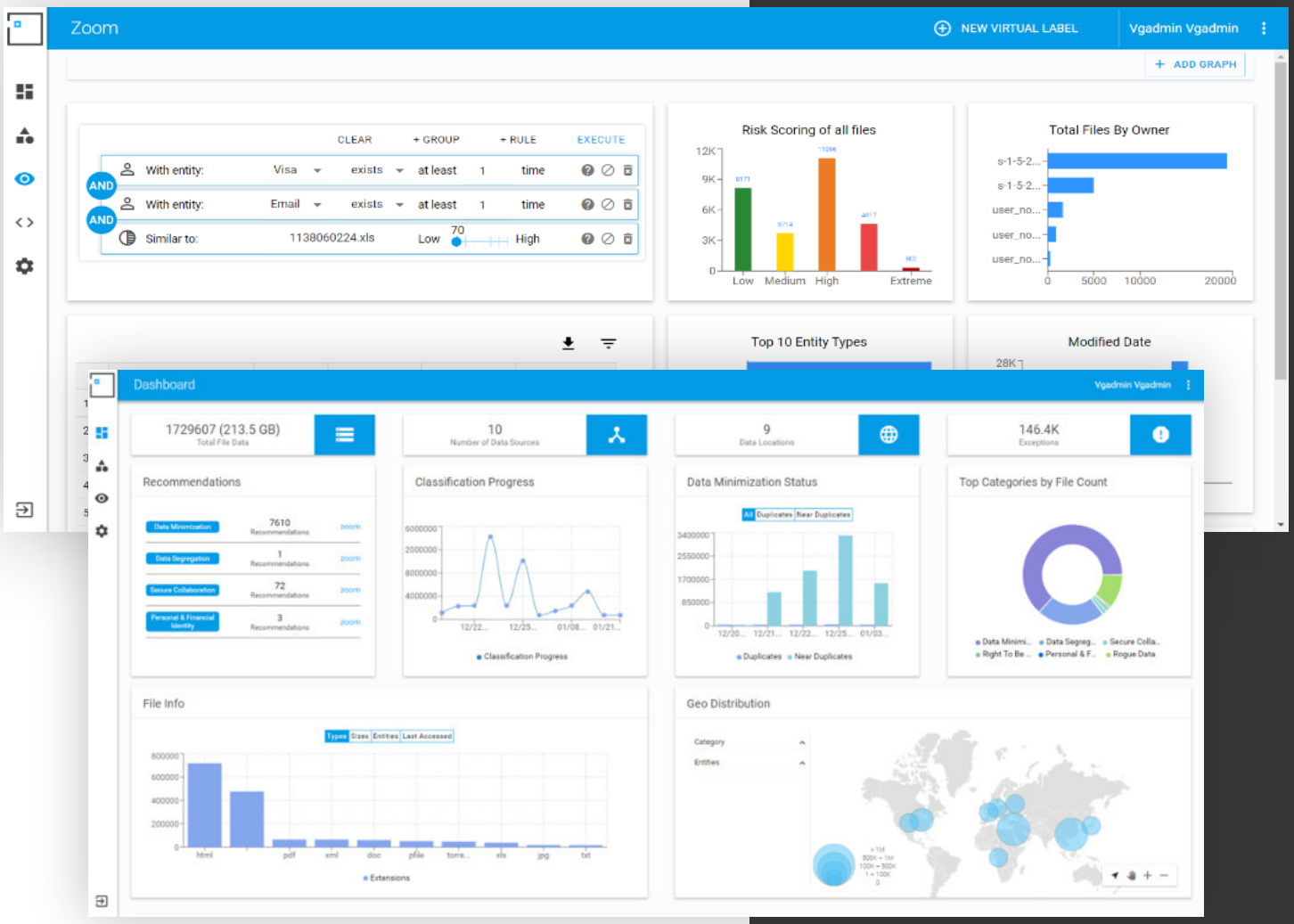
Similarly, to reduce the attack surface and save up to 40% on cloud file processing and storage costs once in the cloud, MSSPs can automate the process of deleting ROT (redundant, obsolete, and trivial) files by using MinerEye's AI-based technology to efficiently scan, categorize and sanitize an organization's unstructured data repository.

4 Data Protection and Secure Shared Collaboration

A cloud environment or a hybrid cloud/on-premise work environment makes data protection a complex task. Once a "nice-to-have", now privacy regulations mandate data protection of sensitive and personal data. MinerEye offers solutions for all these environments, enabling MSSPs to offer customers AI and ML-based automation to identify, group and handle data from multiple perspectives: Complying with privacy regulations, optimizing the business critical data footprint, and securing a brand's assets and reputation.

Protect your Microsoft Environment in a click from the Azure Marketplace

In addition, MSSPs working with customers holding licenses to Microsoft Office 365 have an additional benefit by working with with MinerEye. Upon a simple download from the Azure Marketplace, MSSPs can activate MinerEye's Azure Cloud Application to scan customer repositories and locate data that is either non-compliant, not secured properly or already compromised – together with risk scoring in a free, fast trial. As part of the trial, MSSPs receive automated virtual labeling overlapping data protection and data privacy policies among file data. On all unlabeled or mislabeled files, a risk score is prescribed, resolving business or security policy conflicts often caused by end-user error or unsynchronized compliance requirements.



MinerEye's **EXTRA BENEFITS** for MSSPs:

1. **Data classification oriented for business processes** and more accurate data privacy compliance, protection policy enforcement, and improved data retention policy execution.
2. **Policy modeling** saving MSSP clients significant time and error of manual work, by modeling, simulating and fine-tuning a data privacy policy, while assessing its accuracy and behavior over time, before implementation.
3. **Auto-classifying file versions** for continual identification and classification of files even when changing formats and content, such as mortgage contracts and their scanned PDF versions.
4. **Granular classification** enabling MSSPs to match a file classification system with the organization's business needs, by using flexible classification modeling capabilities (not a rigid 5 label system) that integrates multiple dimensions.
5. **Classification consistency** and scalability even when adding data sources on the fly. MSSPs can maintain uninterrupted, continuous and incremental discovery and classification as the system scales up to scan more data and more distinct sources.

Keeping Data Safe Among Your Customers

Although multi-tenancy supports MSSPs servicing customers for cost and scalability, security issues can often arise with misconfigurations. Organizations look to a MSSP who can protect their data among all customers, maintain each one's privacy, and provide the same level of cyber defense against external threats. By providing customers with cloud data optimization solutions, while fully protecting their data from leaks or disclosure, MinerEye extends MSSPs services to govern their unstructured data for numerous use cases that support each customer's operational goals. When working with MinerEye, MSSPs and clients benefit from continuous monitoring and safeguarding their crown jewels.

Who is MinerEye?

Founded in 2015 by:

- Yaniv Avidan
- Gideon Barak
- Avner Atias

Key Investors:

- AWZ ventures
- Marius Nacht
  Co-Founder and Chairman of CheckPoint Software
- SBI investment

"You can't protect what you can't find. MinerEye finds the data that needs protection."

Gartner Cool Vendor 2016

Cool Vendors in Security Infrastructure Protection Report by Gartner, May 4, 2016

"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"

Will Xiang, Vice President Cyber and Privacy, RICHTER.

www.minereye.com contact: info@minereye.com