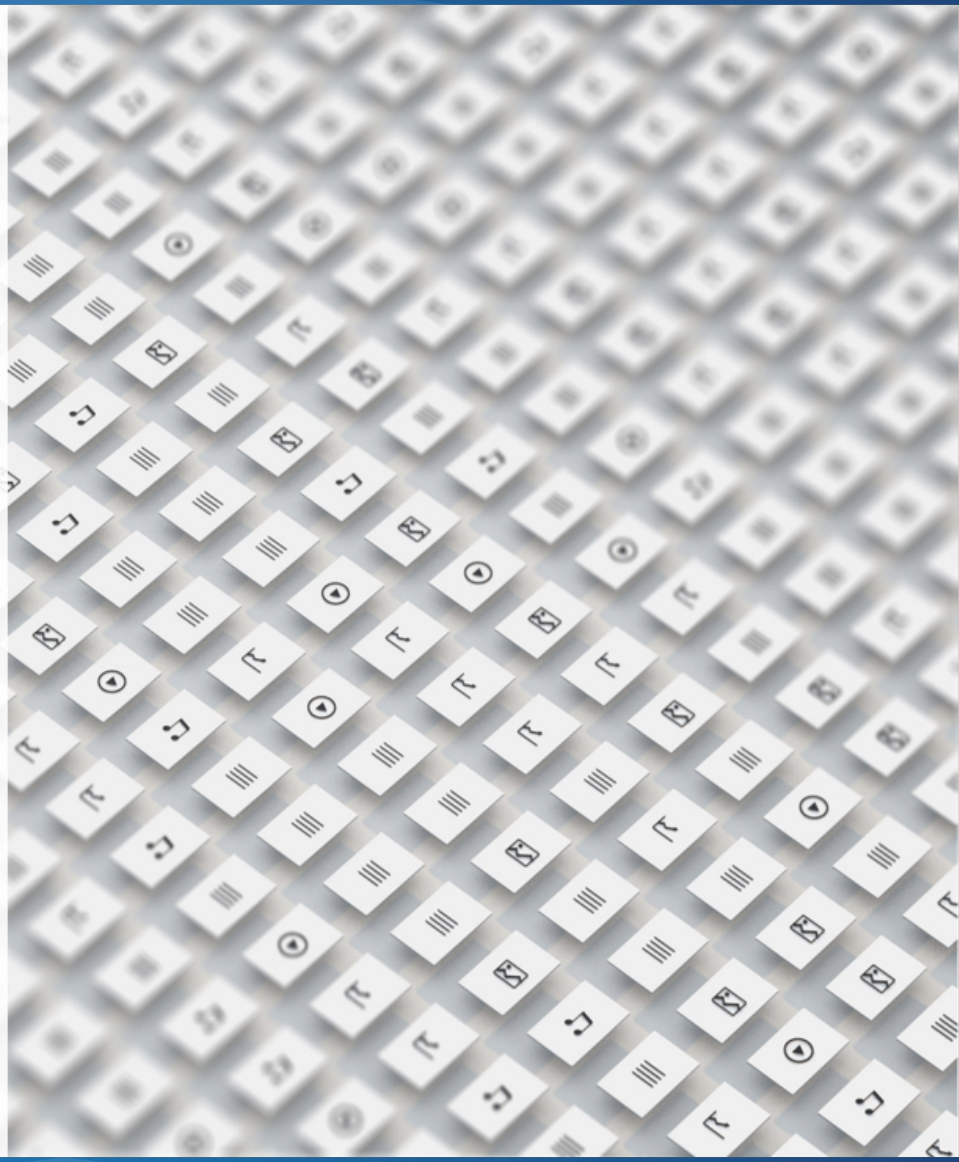
AI-Powered Information Governance



June 2019

IDENTIFY

90%

of data in existence today was produced in the last two years[1]

70-80%

of the data created in the last two years is unstructured, unidentified, uncontained, dark data[1]

CLASSIFY

83%

of organizations store sensitive data in the public cloud[1]

1 in 4

Organizations have experienced data theft from the public cloud *(found for both SaaS and Iaas)* [1]

OPTIMIZE

97%

of organizations use cloud services *(public, private, or hybrid)*[1]

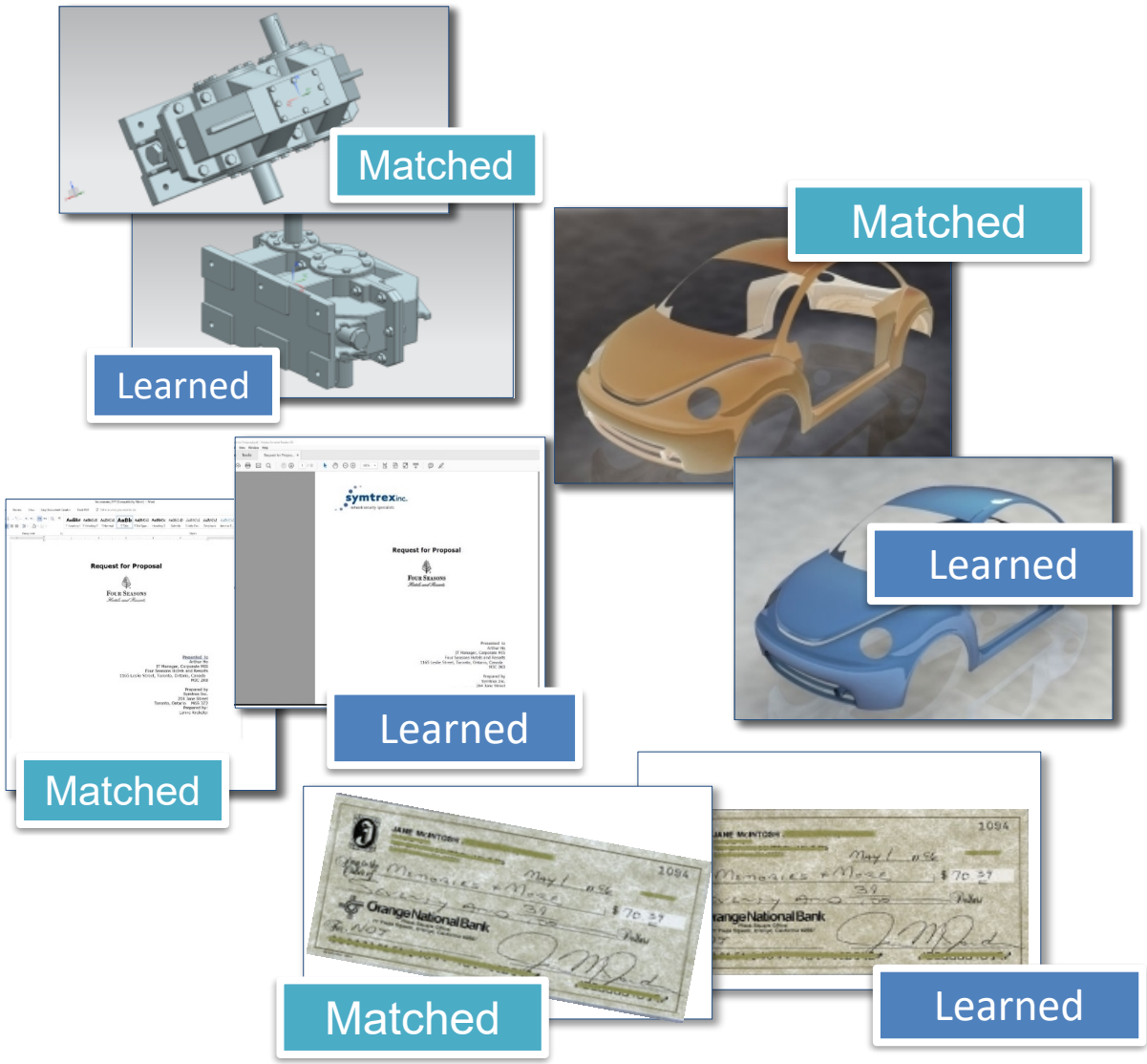
66%

of IT professionals say security is their greatest concern when adopting a cloud computing strategy [2]

Solution Overview

MinerEye interpretive AI™ is a fusion of Byte level pattern recognition and unsupervised clustering of patterns. MinerEye interpretive AI™ uses computer vision to read bytes of an exemplar file and create a signal – a mathematical vector.

The exemplar & its signal *is* the rule



See Beyond Data

Security	Compliance	Tactical Value & Impact	Strategic Value & Impact
• Identify • Analyze • Protect	• Classify • Define • Enforce	• Execute Mission • Enhance Oversight	• Governance • Cybersecurity

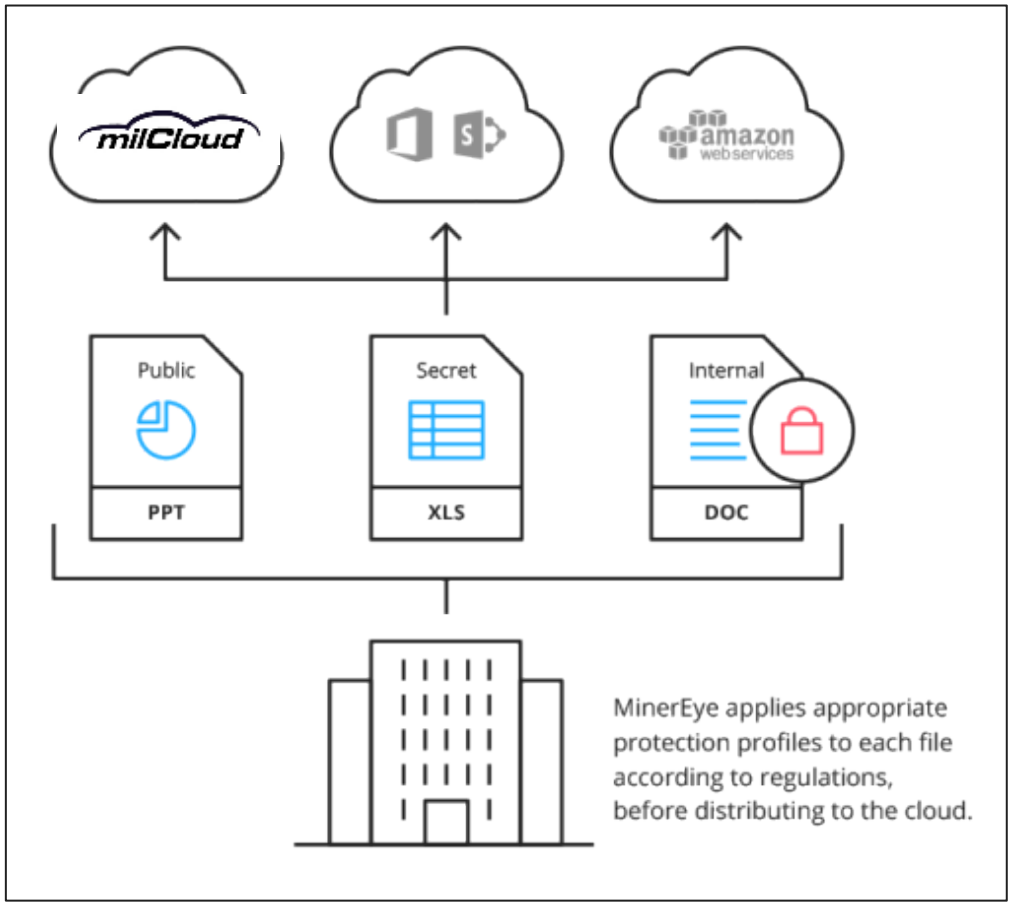
Identification	Locate data to determine infrastructure and enhance data governance
Data Minimization	Remove redundant data in multiple locations to reduce storage and attack surface
Automated Classification	Set sensitivity labels, automatically cluster and track dispersed data
Forensic Analysis	Data spillages, FOIA requests, accidental or malicious release of data
Data Optimization	Minimize data, define criticality levels, provide visibility on-prem and cloud

Preparing for a Secure Cloud Migration

MinerEye stands as a mediator, ensuring the privacy and protection of data that travels between the premise and the cloud, as enabled by hybrid cloud models

Features enable customers to clearly define data impact and criticality categories, segregate one data group from another, establish and apply appropriate protection profiles

This allows for an in depth data analysis that provides deep visibility into infrastructure



Potential Savings

The Association of Information and Image Management (AIIM) reports that on average, half of an organization's retained information has no business value.

The Compliance, Governance, and Oversight Council (CGOC) estimates that a company with 10 petabytes of data could be spending as much as $34.5 million on data that could be deleted.

Site	Storage	Estimated Potential Cost Savings
Army Customer	46.3 TB storage	Estimated **$160k** in redundant data
DoD Customer	288 TB storage	**$994k**
USAF Customer	11 TB storage	**$345k**
Potential Total		**~$1.5M redundant data**

Site	Storage	Estimated Potential Cost Savings
Pentagon	22TB/day 8.03PB/yr	**$28M** in redundant data costs
Potential Total		**~$28M redundant data**

"The Pentagon collects 22 terabytes of data every day…You cannot exploit 22 terabytes worth of data the way we are doing things today."
-Lt. Gen Jack Shanahan, Director, Joint Artificial Intelligence Center, Office of the Department of Defense Chief Information Officer, the Pentagon.

Use Cases

United States Financial Services Group

- Problem – Unknown company proprietary data usage and unidentified ROT data
- MinerEye Solution - located 5 million obsolete documents that customer reduced
- MinerEye Solution - Customer is now utilizing data forensics to analyze dark data worldwide

Worldwide Integrated Circuit Manufacturer

- Problem - Internal Intellectual Property leakage and GDPR & PII compliance
- MinerEye Solution – Identify IP existing outside approved facilities
- MinerEye Solution – GDPR and PII identified and subsequently reduced or protected

United Kingdom Bank

- Problem – Unknown extent of sensitive customer data in business data sets
- MinerEye Solution - found thousands of rogue files that contain sensitive customer data in the form of Excel and Access DB (.mdb) that were subsequently classified and cleaned

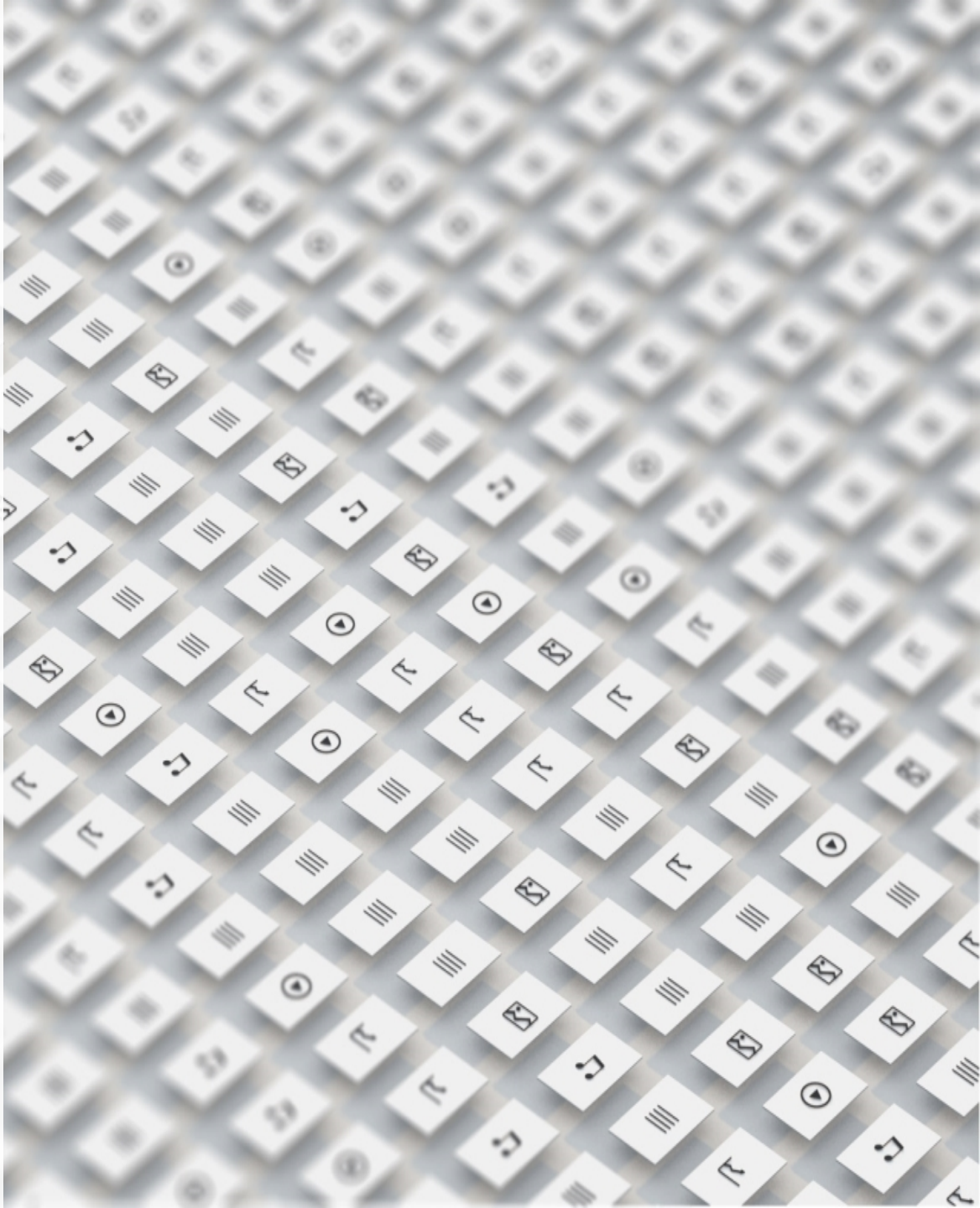
Enterprise Implementation

- Enhanced Cybersecurity
- Operational Efficiency
- Regulatory Compliance
- Risk Management

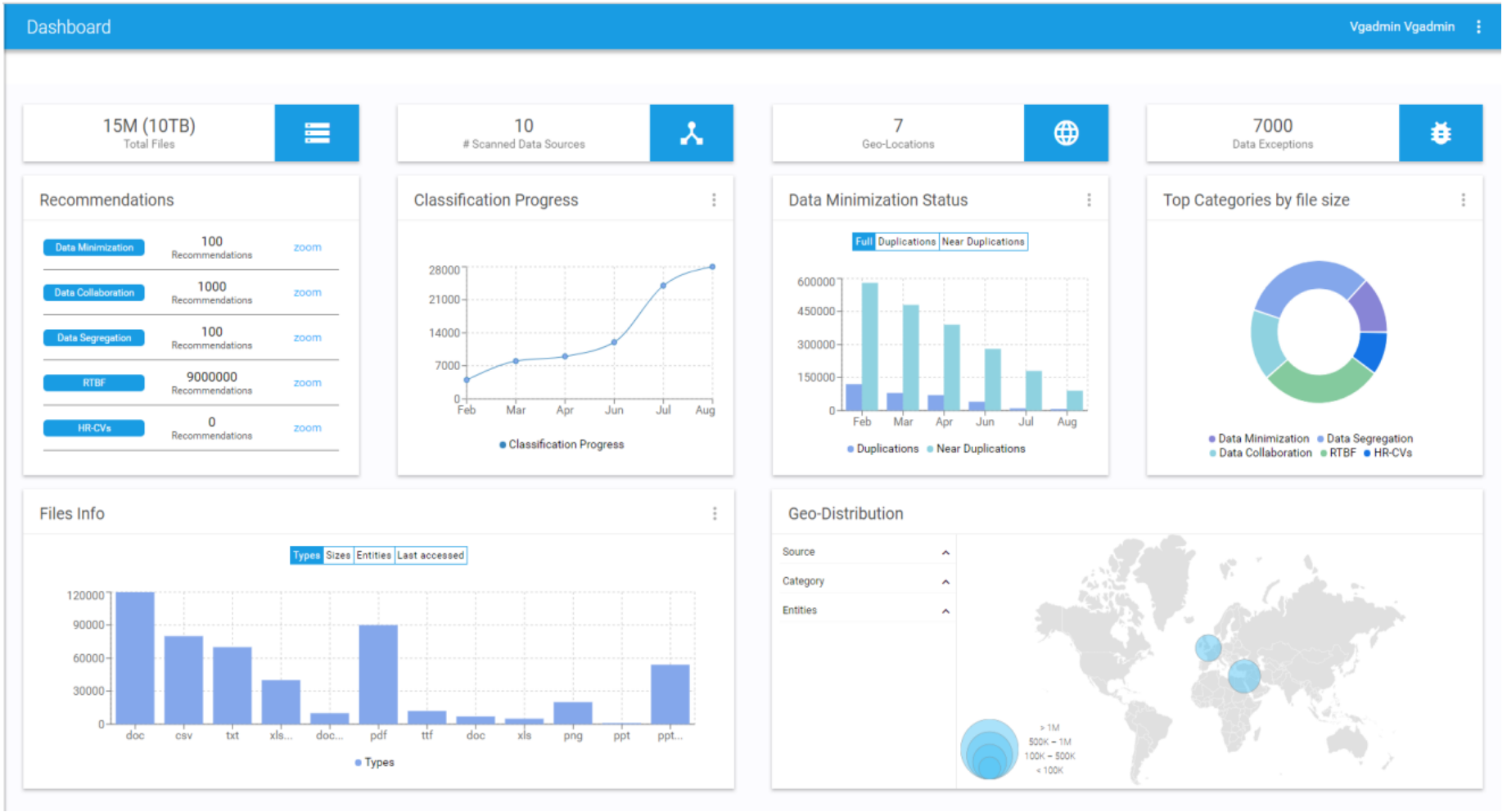
- https://agile-defense.com/services/minereye

minereye

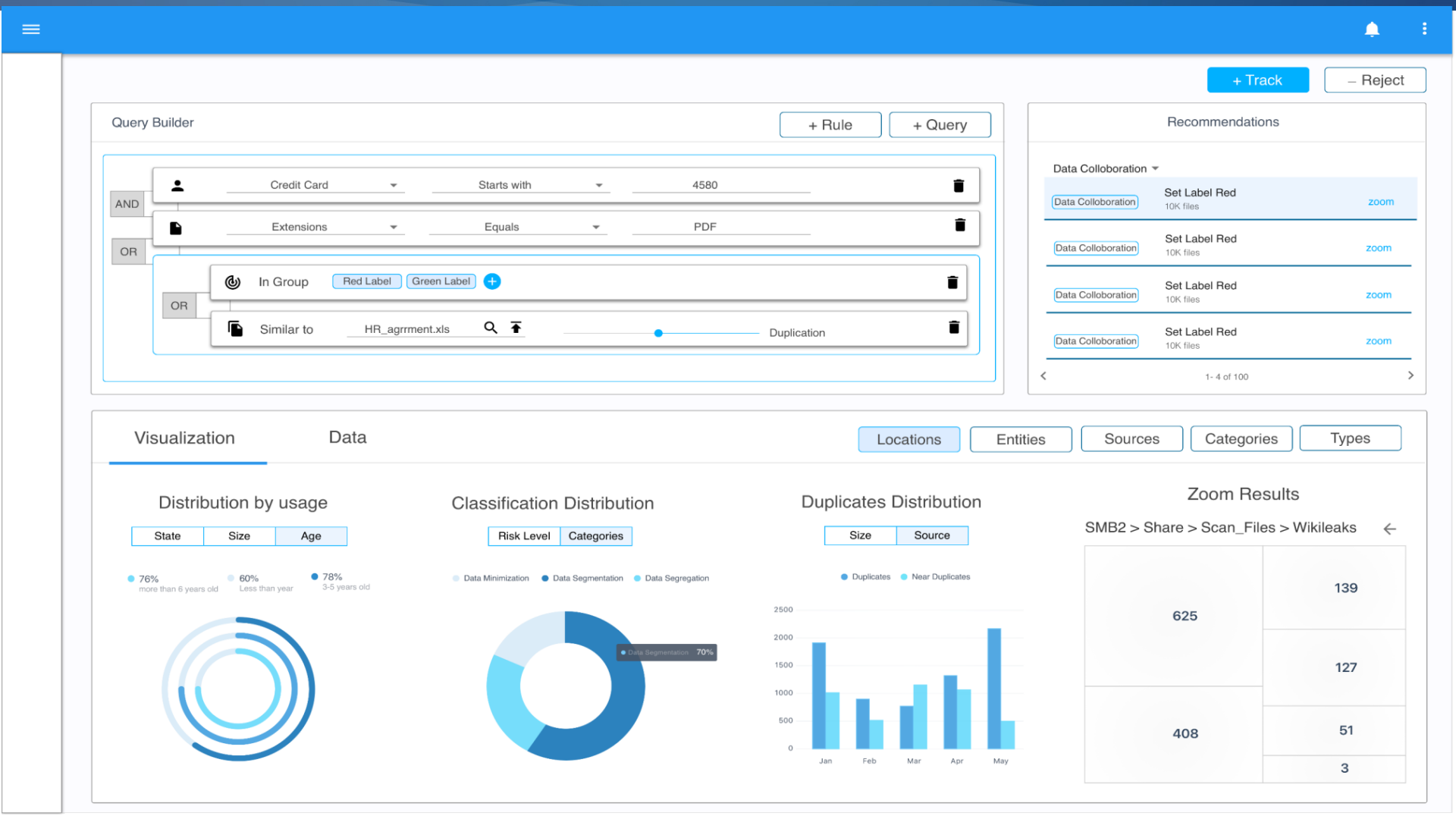
Supporting Documents



MinerEye Data Tracker ™ GUI

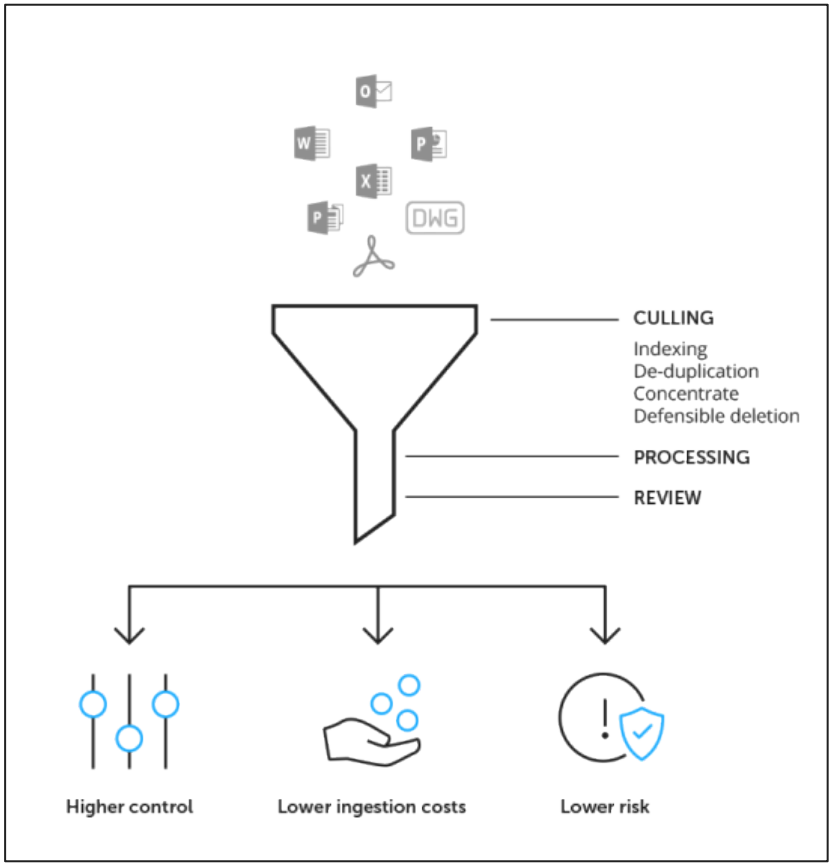


MinerEye Data Tracker ™ GUI



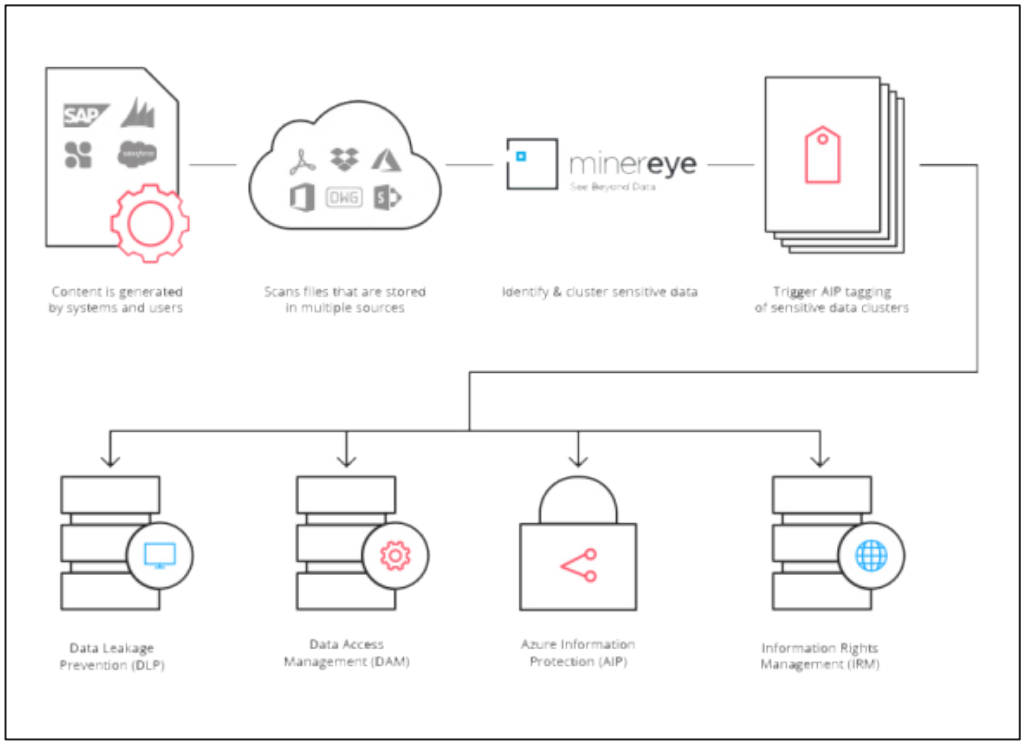
Use Case: Data Minimization

- MinerEye helps companies minimize obsolete and redundant data that has accumulated over time and takes up precious data storage.
- According to the Governance and Oversight Council (CGOC), a company with 10 petabytes of data may reduce storage costs by approximately $34 million by properly disposing of its redundant data.



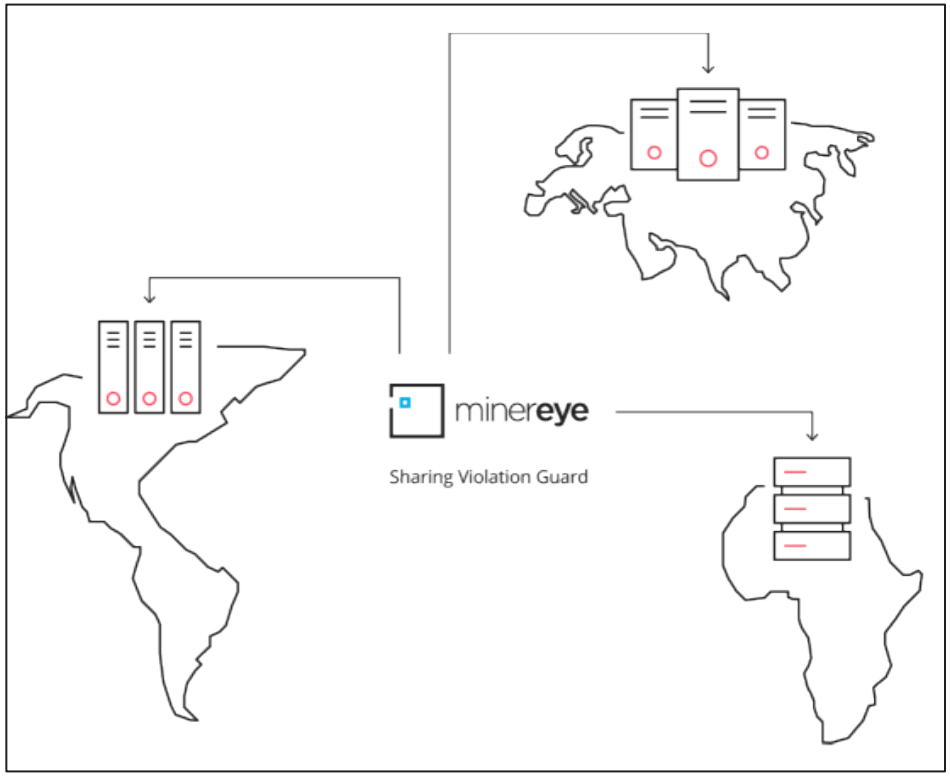
Use Case: Automated Data Classification

- MinerEye tailors automated classification capabilities to your current data protection systems, ensuring consistent and comprehensive classification of all essential data.
- MinerEye's integration with data protection software tools, such as Azure Information Protection (AIP), propagates AIP labels to unlabeled data, and assures comprehensive and efficient data classification and protection.



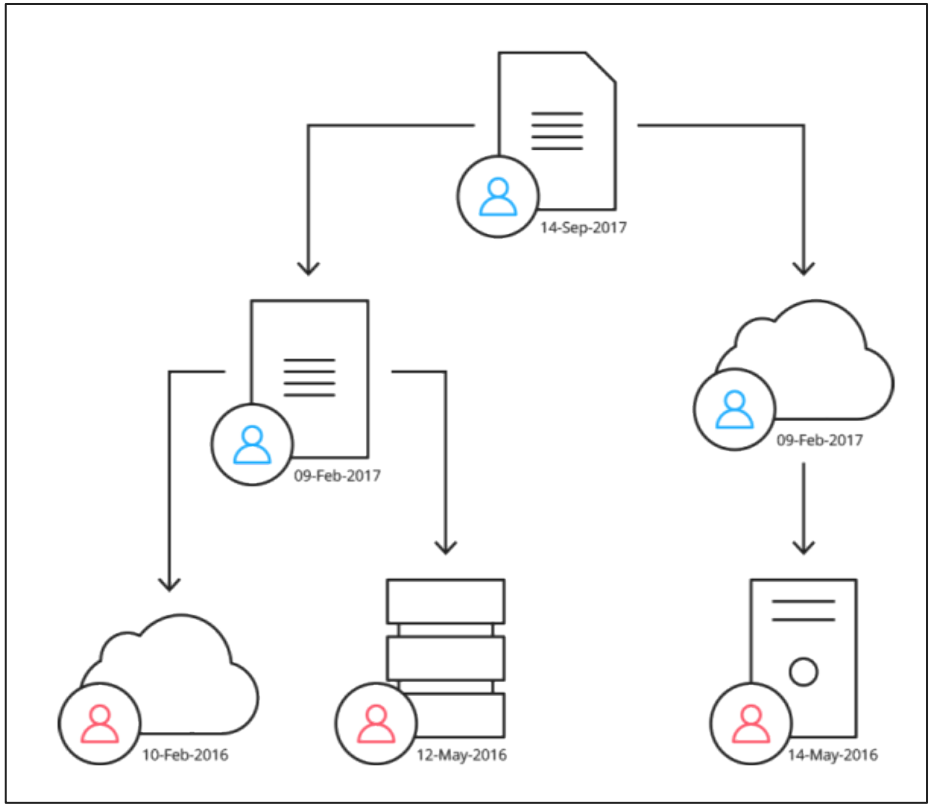
Use Case: Data Segregation

- MinerEye's Data Tracker™ continuously maps and alerts on data segregation issues and data sharing violations that are prevalent among large dataset carriers.
- MinerEye distributed architecture enables companies deploy a net of virtual machines (VM) across company sites, visualizing Data Residency and achieving sovereignty regulation compliance

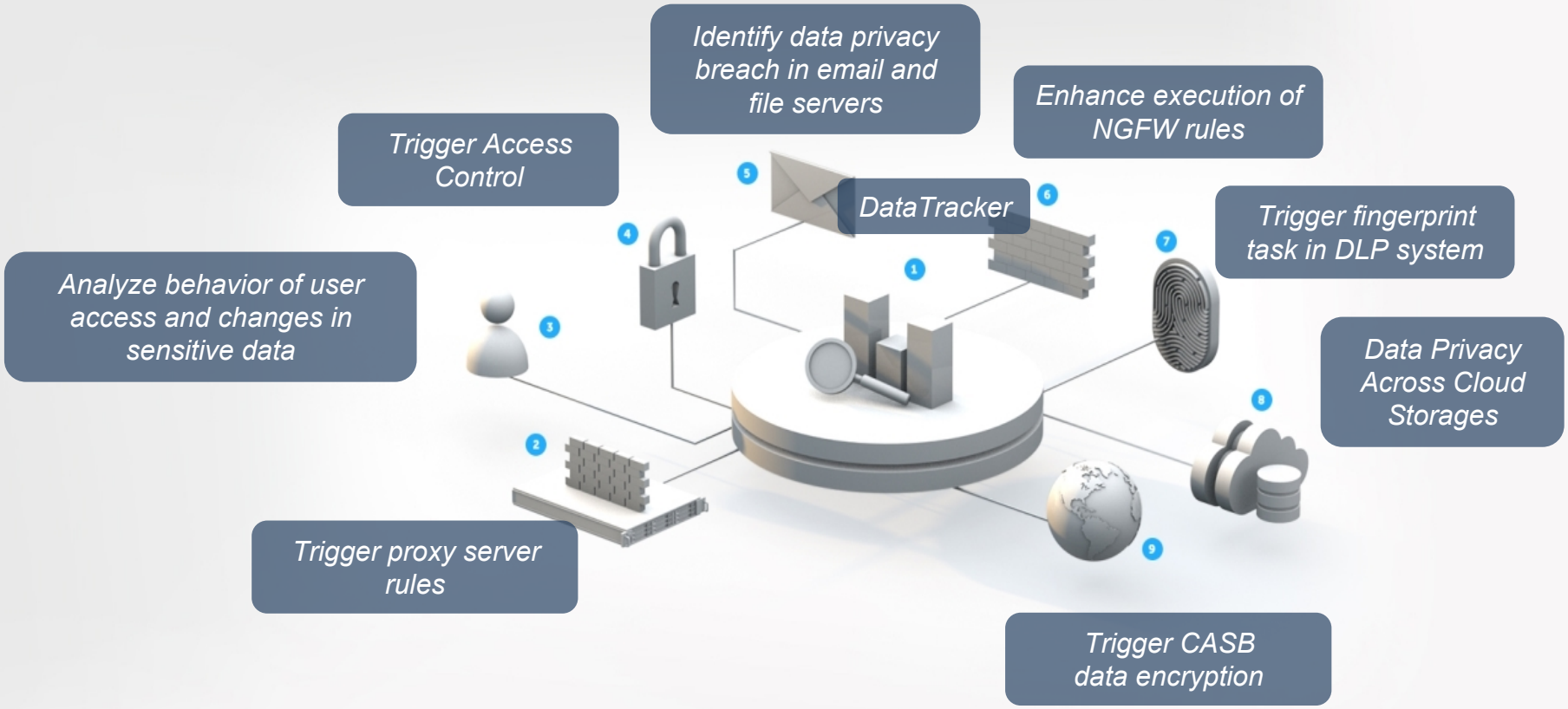


Use Case: Forensic Data Analysis

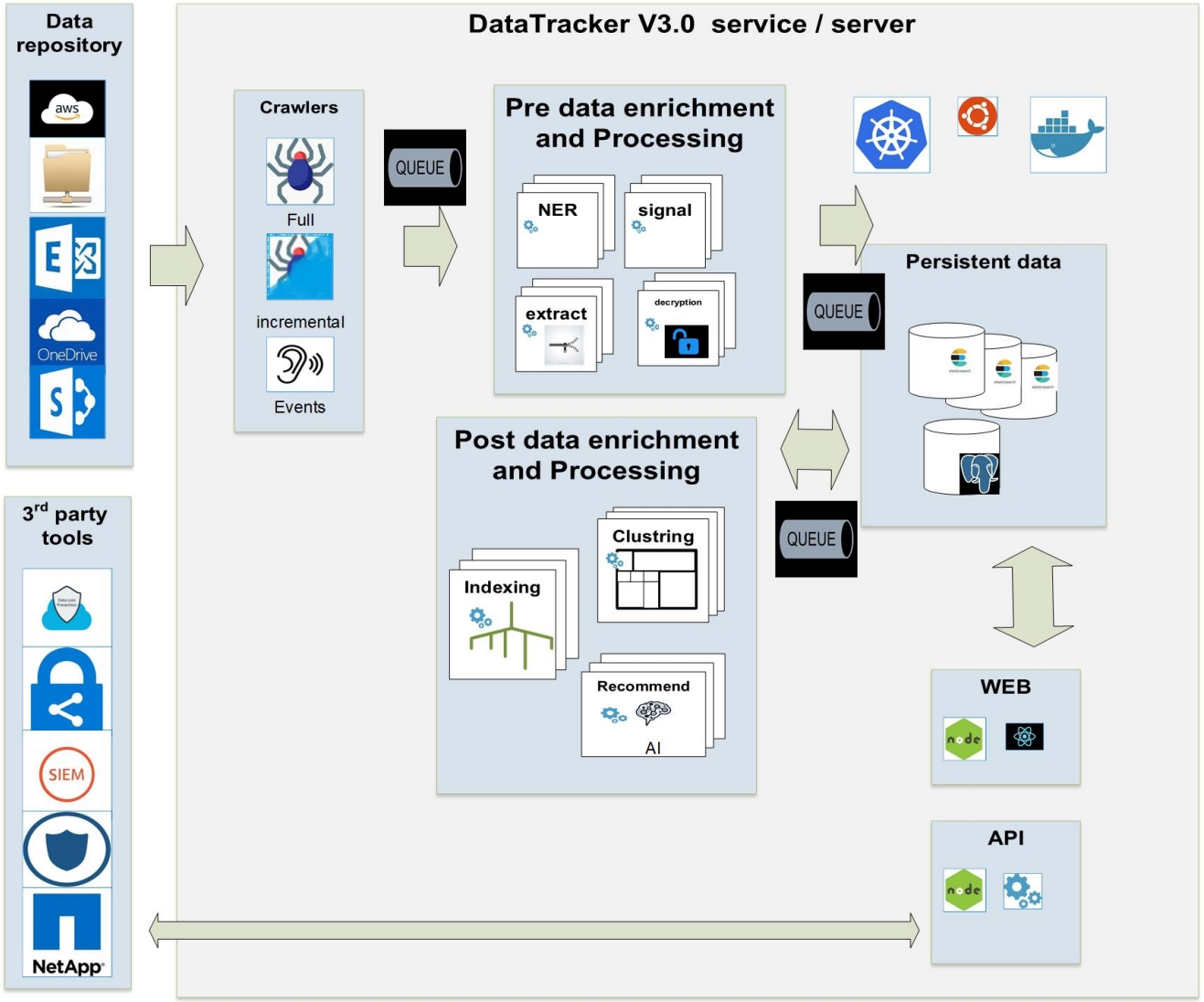
- MinerEye logs data behavior by scheduled scanning of your sensitive information clusters.
- MinerEye can instantly identify and present where your data is or was located at different times, whether it has been modified, who handled it and more.
- MinerEye automates alternative months of manual work to investigate the movement and tampering of data enabling companies to cut time to know and report on data breach according to regulations



AI Architecture



Reference Architecture



Deployment Open Vitrutal Machine

One VM supports up to 120TB source data

Optimal OVA Compute Resources	
CPU	16GHz / 8 Core
RAM	64GB
Disk	2TB