GeoLang Data Technologies
A Shearwater Group plc Company

Datasheet

Ascema Sensitive Data Discovery and Extraction

Locate, analyse, review and extract your sensitive and high-value data

Why Sensitive Data Discovery and Extraction?

Data protection tools can - and should - enhance a human-lead decision making process. Current security solutions typically result in thousands of lines of reports that are then fed into SIEMs which, in turn, churn out yet more data.

Ascema Data Discovery and Extraction offers a powerful solution to what is becoming an increasingly prevalent problem. Instead of ever more lines of reports, sensitive data remediation is provided by end users via elegant alerts and a simple to use dashboard. Highly automated with dual reporting, security teams are now confident that sensitive data is being managed effectively by data owners themselves.

A steady rise in the number of Data Subject Access Requests (DSARs) is adding to the current ‘where’s my data’ problem; increasingly complicated by enormous amounts of unstructured data widely spread across organisational systems. The ability to rapidly locate information across an organisations digital estate and to easily review, collate and extract that data into one central repository, is essential when faced with regulatory time constraints.

The Ascema Sensitive Data Discovery platform accurately locates sensitive data and intellectual property across a multitude of data repositories such as endpoints, servers, external drives, USBs, Office 365, and cloud storage environments including IONOS, AWS and Azure with automated data extraction.

Data Discovery – The First Critical Step Before Data Extraction

Ascema identifies sensitive and regulated data both at rest and in transit. Automated and flexible search task options use a combination of pre-defined rules, bespoke regular expressions, and complex queries.

Data discovery and extraction has never been simpler. Once extracted the repository matches can be easily reviewed in context for further filtering. Sub-searches and compound queries are simple to perform with outputs either to targeted repositories, in the cloud or on premise, as well as being downloadable or exported in a variety of formats.

Enterprise reporting via user-friendly dashboards and the dynamically generated Data Discovery Executive Summary (HERO Report) provide additional data visibility to ascertain data threat patterns and user activity in real-time and offer flexible remediation options such as alert, quarantine or remove.

Key Features

Simple and elegant to deploy and use

Highly automated remediation capabilities

Easy data discovery and extraction

Dynamically generated board level reporting

Ascema Sensitive Data Discovery

- Pre-configured and customisable search patterns
- Compatibility with Windows, Linux, MacOS and cloud including AWS, Azure, Google, Office 365, Exchange and SharePoint
- Comprehensive data monitoring both at-rest and in motion
- Automated and flexible end user or administrator remediation
- Active, passive, stealth and forensic modes

Ascema Sensitive Data Extraction

- Search and extract unstructured data
- Quickly review results in context for further filtering
- Extract individual files with sensitive data from container files
- Filter results and create further repositories and sub repositories
- Target repositories or download in a variety of formats
- Unified search and reporting interface for Endpoints, File Servers, Alfresco and O365 apps
- Export to SIEMs e.g. Splunk
- Easily create new tasks based on previous tasks
- Pattern specific default confidence levels lowers false positives

Key Benefits

Gather deep and actionable insights into your sensitive data

Complete data visibility across your digital estate

Automatically alert users to sensitive data stored across the enterprise and apply appropriate remediation

Support regulatory compliance and standard requisites through automated sensitive data discovery and extraction

Secure data through the real-time application of protective controls including sync folders and USBs

Continuous and comprehensive data monitoring

Understand your organisations sensitive data risk posture

Supports digital and data transformation processes