GeoLang
A Shearwater Group plc Company

Ascema Sensitive Data Discovery

Sensitive and high-value information discovery across your entire digital estate

Why Do We Need Sensitive Data Discovery?

With over 40% of businesses being uncertain as to the whereabouts of their sensitive information, and experts forecasting a 4,300% increase in annual data generation by 2020, the ability to locate, control, and protect our most vital information has become an overwhelming priority.

With a dearth of solutions on the market, often reporting on thousands of instances of data found, data security analysts cannot possibly keep up and thus the value and return on investment (ROI) of these tools is brought into question.

Organisations today are being subject to even stricter data protection requisites, including data subject access requests, than ever before — bolstering data protection and security as an ongoing obligation requiring demonstrable compliance. Yet, with over half of businesses having no fixed method in place for responding to such regulatory requests, and the numbers of reported data breaches continuing to escalate, businesses find themselves in an ever-precarious situation that could potentially lead to litigation, investigation, and, perhaps most cripplingly, financial penalties.

Recent years have also seen a considerable increase in the numbers of remote workers, with the Office of National Statistics predicting half of the UK workforce to be working virtually by next year, and businesses are relying heavily on cloud-based storage and file sharing systems to manage and share vast amounts of corporate information more seamlessly. These new capabilities — enabling employees to create, access, and store data across a multitude of corporate repositories— poses a significant challenge to businesses in ensuring the management, protection, and confidentially of their critical data is maintained.

Architecture

Ascema Sensitive Data Discovery accurately locates and secures the movement of sensitive data and intellectual property across a multitude of data repositories comprising, but not limited to, endpoints, servers, external drives, cloud applications, such as Office 365, and cloud storage environments including IONOS, AWS, and Azure.

Offering automated and flexible search task options created using a pre-defined set of rules, encompassing data protected under GDPR, PCI, or HIPAA, as well as supporting more complex queries in the form of Compound Search Tasks to identify data sets specific to the organisation, the Ascema Sensitive Data Discovery tool identifies sensitive and regulated enterprise information both at rest and in transit.

Bringing the enterprise employees into the equation is a must for those organisations who are looking to gain true ROI as well as organisational resilience. Ascema reports data found on endpoints and in file shares to the end user for remediation – significantly lessening the load on data security analysts.

Enterprise reporting, obtainable through user-friendly dashboards and the dynamically generated **Data Discovery Executive Summary (HERO Report)**, also provides comprehensive data visibility to ascertain data threat patterns and user activity in real-time, identifying any potential policy violations, whilst also offering flexible remediation options.

Deployment

The Ascema Sensitive Data Discovery solution consists of two simple components:

Ascema Endpoint Manager

This provides a user interface to manage Search Tasks, including devices, users, licence and other areas of Ascema, and is shipped as an .exe file. The minimum requirements are a Windows 7+ machine with 4GB of memory and 2 CPUs, as well as the latest versions of Chrome or Firefox.

Ascema Endpoint Agent

This should be installed on each of the monitored endpoints, and is available for Windows (.msi), Mac (.pkg) and Linux (.rpm, .deb.). Windows agents can also be deployed on Windows Server 2012+ to search file servers, as well as being configurable to search Office 365 apps and Alfresco repositories, and the .msi files can be deployed using client installs such as GPOs and SCCM. The Manager's IP address or Host name can be provided to the agents at install time, as well as being auto discoverable through UDP.

Both the Manager and Agents do not require any publicly accessible ports on the internet and can be deployed both on-premise and in the cloud.

Sensitive Data Discovery Executive Summary - HERO Report

The high-level **Data Discovery Executive Summary**, designed for configurable and periodic reporting on key data risks and mitigations within the organisation, is easily generated as a PDF or in html format for editing to, not only alleviate these data risks by locating sensitive information in real time, but also efficiently report the ROI, support the business case for further resources and digital transformation projects.

GeoLang consultants can also augment the dynamic report with 'work packages', detailing key findings and recommended actions for remediation – including training and policy development.

Features

Designed to perform automated sensitive data discovery on a one-time, regular, quarterly, or annual basis, depending on business requirements, the Ascema Sensitive Data Discovery solution provides:

One-time rapid deployment	Easy and agile to deploy, configure, and manage, negating the overheads from overly convoluted products and services
Pre-configured and customisable discovery patterns	Search Tasks can be created using a predefined set of rules, whilst also supporting the configuration of more complex queries in the form of Compound Search Tasks as well as the ability to enter bespoke regular expressions.
Seamless integration and accessibility	Compatibility with an extensive range of operating systems, including Windows, Linux, MacOS and cloud including AWS, Azure and Google as well as Office 365, Exchange mailboxes, and SharePoint, to ensure fast and easy searching across your digital estate.
Comprehensive data monitoring both at-rest and in motion	Complete quick and accurate data-at-rest discovery across various digital storages, whilst the Real Time Protection Search Tasks feature with built-in alerting and tracking capabilities provides visibility into sensitive data in transit including on USBs.
Central reporting dashboard	User-friendly dashboards are available in one central location, providing both data analyst and end users with essential oversight into the location and risk status of their sensitive data with real-time reporting.
Sensitive Data Discovery Executive Summary	A dynamically generated board-level overview of data discovered, captures mitigated data risks and return on investment (ROI), to provide essential visibility and reporting into sensitive data across your organisation.
Automated and flexible remediation:	Information can be quarantined and deleted for PCI DSS compliance, as well as being compiled in a repository to support activities required to comply with the General Data Protection Regulation (GDPR) and DSARs where appropriate
Information classification functionality	Detect and label sensitive data in Alfresco with the appropriate sensitivity to ensure compliance regulations are demonstrably met, as well as prevent sensitive information from being stored outside dedicated enterprise locations.

GeoLang Limited, Cardiff Business Technology Centre, Senghenydd Road, Cardiff, CF24 4AY
P: +44 (0) 2920 647012 E: contact@geolang.com