GeoLang Data Technologies
A Shearwater Group plc Company

Frequently Asked Questions (FAQ)

Ascema Sensitive Data Discovery

What is Ascema Sensitive Data Discovery and how is it different to other technologies?

Ascema Sensitive Data Discovery utilises content analysis to automatically locate, control, extract, and remediate sensitive and regulated information - including confidential and protected data such as personally identifiable information (PII), payment card industry (PCI) data, Intellectual Property (IP) and HIPAA - across multiple data repositories in a single platform.

Elegant and simple to deploy, the Ascema Sensitive Data Discovery tool locates and filters data into a usable, valuable and exportable resource to help organisations with compliance, data protection and end user training; simple deployments can be up, running and producing results often in less than half a day.

Automated reporting, available through user-friendly dashboards and the dynamically generated Data Discovery Executive Summary, our 'HERO Report', enables users to ascertain data threat patterns and user activity in real-time, identifying any potential policy violations, whilst also offering flexible remediation options to protect and extract data appropriately.

How does Ascema Sensitive Data Discovery actually work?

With a small footprint, our unobtrusive Ascema Endpoint Agent is installed on endpoints, servers and connected to cloud applications. The central Ascema Manager communicates tasks to the Ascema Endpoint Agent controlled internally by the organisation. Ascema Agents service the Manager by executing search and extraction tasks either on demand or at predefined schedules.

What systems are compatible with Ascema Sensitive Data Discovery?

Ascema Sensitive Data Discovery is compatible with an extensive range of operating systems, including Windows, Linux, and MacOS, as well as seamlessly integrating across a multitude of data repositories including, but not limited to, endpoints, servers, external drives, cloud applications, such as Office 365, S3 Buckets and Alfresco.

Events can be pushed to external SIEMs including Splunk, ArcSight, and IBM i2 Analytics, to assist in the monitoring and analysis of discovered data residing across your digital infrastructure.

What types of sensitive data can be detected?

Offering automated and flexible search task options using either pre-defined or bespoke rule sets, including GDPR, PCI, or HIPAA, Ascema also supports more complex queries in the form of Compound Search Tasks. Ascema Sensitive Data Discovery searches unstructured datasets stored in numerous formats across the digital estate.

Ascema Sensitive Data Discovery also includes the following set patterns:

PCI
making sure organisations know where their payment card data resides

GDPR
identifies and protects the personal data and privacy of EU citizens, Ascema assists with GDPR compliance.

HIPAA
identifies and protects an individual's health records in unstructured data and other personal health information

Can I complete a sensitive data discovery search task in real-time?

The Ascema Sensitive Data Discovery solution discovers, protects and extracts sensitive and regulated enterprise information both at rest and in real-time.

The Real-time Protection task feature within the system allows users to manage the movement of their sensitive data in transit, alerting the end user and system administrator in real time. Highly automated remediation actions, as part of the process of resolving and managing the presence of sensitive data, include the ability to quarantine.

How do I complete a data retrieval task using Ascema Sensitive Data Discovery?

Following the initial data discovery search phase, Ascema Sensitive Data Discovery can extract identified data in numerous file formats, including email, from their original location and create a centralised repository either on premise or in the cloud. Users can also further refine a repository with the ability to filter the extracted data. The extracted data can be viewed on the server or seamlessly downloaded in the original file format, alongside being exported as a summary file in multiple formats, including HTML, CSV, and XLSX.

How does Ascema Sensitive Data Discovery support remediation?

Bringing the data owner into the remediation process is a powerful tool. Ascema's highly automated workflow supports end user remediation and training as well as administrator lead quarantine and delete options.

Ascema Sensitive Data Discovery can also detect and visibly classify sensitive data in Alfresco to support both end user education and data loss prevention.

What reporting options are available in Ascema Sensitive Data Discovery?

The high-level Data Discovery Executive Summary ('HERO Report'), designed for configurable and periodic reporting on key data risks and mitigation within the organisation, is easily generated as a PDF or in html format for editing. Available at the touch of a button, the HERO Report elegantly and simply reports Return on Investment (ROI) for both the tool and the implementation team whilst also supporting the business case for further resources and digital transformation projects.

User-friendly dashboards are also available in one central location, providing users with essential oversight into the location and risk status of their sensitive data, as well as providing real-time reporting to administrators and departmental heads.

How is Ascema Sensitive Data Discovery deployed?

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 8GB of memory and 2 CPUs, as well as the latest versions of Chrome or Firefox. Also available as Sub-Managers that can be deployed in different geographical locations within the enterprise version.

Ascema Endpoint Agent

Easily deployed and installed on each of the monitored endpoints and available for Windows (.msi), Mac (.pkg) and Linux (.rpm, .deb.), Windows agents can also be deployed on Windows Server 2012+ to support file servers, available as an app for Office 365 and Alfresco; .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, in the cloud or as a hybrid solution.

Pre-Deployment

- Schedule deployment date
- Identify estate
- Allocate Ascema resource
- Identify Sensitive Data Discovery tasks

Step 1

- Deploy Ascema Sensitive Data Discovery
- Schedule Sensitive Data Discovery tasks
- Begin data audit

Step 2

- Ascema immediately starts passive tasks
- Interim reports are available within the UI
- Data can be exported for further analysis

Step 3

- Review task results
- Switch on live remediation and monitor if required
- Edit search tasks as necessary

Post-Deployment

- Presentation of Reports

Do users need to be authenticated when using Ascema Sensitive Data Discovery?

The system authenticates user identity through a combined username and password login.

Can GeoLang see or store any of my data via the Ascema Sensitive Data Discovery system?

We do not hold or store any of your data since we do not have any access or visibility to the tool utilised by the organisation.

Where can I learn more about Ascema Sensitive Data Discovery?

You can contact Team GeoLang at **geolang.com/contact-us** to request a free demonstration with one of our top technical engineers. Review our online user guide pages and product brochures for more information by clicking on the links below:

- User Guide: **docs.ascema.com/endpoint/latest**
- Ascema Sensitive Data Discovery and Extraction: **Datasheet**
- Ascema Sensitive Data Discovery: **Scan-as-a-Service**
- Sample Data Discovery Executive Summary: **HERO Report**

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