GeoLang Data Technologies
A Shearwater Group plc Company

Frequently Asked Questions (FAQ)

Ascema Data Loss Prevention (DLP)

What is Ascema Data Loss Prevention, and how is it different to other technologies?

GeoLang's Ascema Data Loss Prevention (DLP) platform is a highly automated, easy to deploy solution for the monitoring, classification and real time protection of confidential and sensitive information at true content level across enterprise authorised applications – on premise, in the cloud or hybrid.

Utilising our patented fingerprinting, classification, and machine learning algorithms, Ascema offers a seamless and transparent end user and enterprise experience designed to support everyday workflows – all without disrupting user productivity. Content fingerprinting ensures protection is enforced regardless of whether users change the file name or type, cut snippets out or recreate within separate applications.

Effortless to deploy and manage, enabling comprehensive data protection from a single dashboard, the Ascema DLP platform is readily integrated with any bespoke or proprietary application – including Office 365, Exchange, Confluence, Google Drive, Box and Alfresco – to ensure rapid and reliable sensitive data transmission across the enterprise.

How does Ascema Data Loss Prevention actually work?

The Ascema DLP platform comprises three separate engines; the patented fingerprinting engine that generates fingerprints, indexes, and performs lookups, a machine-learning algorithm that provides the automated classification function and a pattern matching engine to recognise sensitive datatypes. The Ascema search capability is facilitated by the core fingerprinting algorithm that recharacterizes text for purpose and produces irreversible content fingerprints that are added to the vault in real time.

Ascema then matches these protected irreversible fingerprints against the content being processed within enterprise applications – intervening when a match is detected – and applying the appropriate remediation according to pre-determined intervention levels, with audit logs and reporting as standard.

How is Ascema Data Loss Prevention deployed?

Ascema DLP facilitates fast, flexible, and effortless deployment to minimise workflow and business disruption. The system can be easily deployed on premise and in the cloud – private and public, or as a hybrid – to prevent unauthorised data sharing within and outside the organisation's network.

The solution can operate as a standalone product or be paired with the Ascema Data Discovery and Extraction solution to locate, monitor, and extract sensitive content stored across the enterprise.

Can Ascema Data Loss Prevention protect my sensitive data as it is being created or shared?

Ascema DLP protects sensitive content throughout its data lifecycle; monitoring data as it is being created, as well as protecting data in transit – and flagging unusual or suspicious user activity – within enterprise authorised applications through comprehensive content analysis.

What are some of the benefits of deploying Ascema Data Loss Prevention?

The Ascema DLP solution boasts a number of key and distinctive benefits:

- ✓ Protects and prevents unauthorised data misuse and sharing of sensitive content in the enterprise and extended supply chain
- ✓ Scans files and data streams to detect, classify, protect, remediate, and report on high value content, including files shared through online collaboration, and email
- ✓ Operates at content level within the document file structure, thus protecting against extracted information attacks (“cut & paste”) across disparate systems such as email and the cloud
- ✓ Uniquely conducts the content-matching process on irreversibly encrypted data, in computer memory; we don’t share the secret to find the secret
- ✓ Guards against the disclosure of common private information types, such as national IDs, PII and credit cards
- ✓ Supports a common business workflow – recognising, for example, corporate workgroups, and triggering protection when members attempt to share sensitive content outside of their group or enterprise
- ✓ Automatically designates documents as sensitive based on business purpose; applying machine learning to recognize common forms, e.g. HR forms, payslips, CVs, contracts, and automatically applies the appropriate real time protection of content

Can Ascema Data Loss Prevention operate in “passive mode”?

Yes, we can! Ascema DLP can passively monitor, track and report on sensitive content.

What platforms does Ascema Data Loss Prevention support?

Ascema DLP integrates seamlessly with enterprise authorised applications and environments including, but not limited to, Office 365, Exchange, Confluence, Google Drive, Box, SharePoint, Alfresco and Windows File Servers as well as being readily integrable with SIEM tools, such as IBM QRadar and HP ArcSight.

Ascema can also extend classification from traditional labelling to content level protection – regardless of file name e.g. Bolden James or Titus classifications. Application level integration using connectors also means coverage is provided regardless of where the application is accessed– at home, at work on mobiles or tablets or even when travelling – and irrespective of which network was used to access the application.

How does Ascema Data Loss Prevention support remediation?

Ascema DLP supports flexible remediation in real time – including track, alert, quarantine and block sharing, both outside of a named set of collaborators or outside the organisation's domain(s) – whilst empowering and educating end users on appropriate data usage; mitigating the risks of data loss through theft, mismanagement and end user error.

There is also no reliance on document tagging for classification so organisations can deliver enterprise-level solutions without the extensive overheads, as well as being able to extend external document classifications to protect the content. No in-document tagging means hackers cannot easily identify your organisations crown jewels!

TRACK — ALERT — QUARANTINE — BLOCK SHARING

What reporting options are available with Ascema Data Loss Prevention?

The Ascema DLP platform delivers granular reporting on a single user-friendly dashboard, providing a comprehensive list of documents scanned and the remedial actions conducted, as well as behavioural analysis - alerting administrators to potential 'Users of Concern' that are exhibiting some unusual activity or generating a large number of events.

Events can be pushed to any external SIEM - including Splunk, ArcSight, and IBM i2 Analytics, to assist in the monitoring and protection of sensitive enterprise information.

How is Ascema Data Loss Prevention (DLP) licensed?

A variety of business models are available based on the number of users with substantial savings on multi-year contracts.

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-set once deployed by your organisation.

Where can I learn more about Ascema Data Loss Prevention?

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

- Ascema Data Loss Prevention: **Overview**
- Ascema Data Loss Prevention: **Datasheet**
- Ascema DLP for Office 365: **Video Demonstration**
- Ascema DLP for Alfresco: **Video Demonstration**