GeoLang Data Technologies
A Shearwater Group plc Company

Elegant, Powerful and Unparalleled Content Level Protection

Empower Employees to Protect Corporate Data and Enforce Security Policies

With businesses relying more heavily on file sharing platforms and collaboration tools than ever before, as well as both consumer preference and enterprise needs driving the creation of more real-time information, the ability to maintain and protect our critical data and corporate crown jewels is both crucial and challenging.

Whilst the rise of cloud commuting has indeed enhanced both productivity and data access, the lack of oversight into managing our employees, as well as the security of our IT infrastructures and applications, can pose a significant threat in terms of resilience, permanence and competitive edge.

Digital data can now be found everywhere; which, when combined with the many ways data can leave an organisation, further amplifies the threat of unintentional data sharing, misuse and exposure; leading to increased regulatory and auditing noncompliance - and, by that extension, fines and civil penalties – as well as compromising Intellectual Property (IP), brand, reputation and thus stakeholder value.

In order to effectively manage and protect our greatest data assets, therefore, it is important to implement a solution that can prevent the unauthorised loss and disclosure of sensitive information throughout its data life-cycle – employing powerful content analysis to accurately automate the classification of and protect sensitive data in real-time – whilst effortlessly monitoring and enforcing compliance with industry and government regulations. At GeoLang, we have got you covered.

GeoLang's Ascema Platform is a highly automated, easy to deploy and use solution for monitoring, classifying, and protecting confidential and sensitive information at true content level across enterprise authorised applications – on premise, in the cloud or hybrid.

Award Winning and Accurate Content Level Protection

Utilising our patented fingerprinting and classification and machine learning algorithms to protect critical content across your digital estate in real time, the Ascema platform offers a seamless and transparent end user and enterprise experience designed to support everyday workflows - 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.

Integrable with popular and approved enterprise connectors, including:

Office 365   box   Exchange   Confluence   Google Drive   Alfresco   Windows Server

Rapid Remediation to Control and Protect Data Throughout Its Lifecycle

Flexible remediation actions in real time include track, alert, block sharing both outside of a named set of collaborators or outside the organisations domain(s) and quarantine. There is also no reliance on document tagging for classification so you can deliver enterprise level solution without the extensive overheads whilst also being able to extend external document classifications to protect the content.

Fast and Flexible Deployment Across the Digital Workplace

Integrating directly at application level into every day tools such as O365, Alfresco, Box and Confluence means coverage is provided regardless of where the application is accessed – at home, at work or even when travelling; central configuration and management for complicated environments are simple to deploy easier than ever before!

Automated Policy Enforcement

Tracking, reporting and enforcing data policies, such as restrictions, are automatic interventions based on content. Machine learning data analytics can further highlight unusual data sharing within a network in real time.

Key Features

Highly automated, elegant and simple to deploy solution for classification and real-time protection of enterprise IP and sensitive data

True content level protection to safeguard sensitive and high-value information throughout its lifecycle – at rest or in use

Enables visibility and control of sensitive information across enterprise applications – including on premise, in the cloud and hybrid, in a single console

Automatically track, report and enforce data policies - with the ability for each data classification to have its own remediation

Granular reporting provides in-depth knowledge to detect, remediate and prevent potential breaches

Empower and educate end users to handle sensitive information appropriately

.

Flexible remediation from track and alert, to block sharing and quarantine whilst also offering the capability to reapply restrictions would data be copied and pasted into new documents or emails

Key Benefits

Prevents the accidental disclosure and misuse of confidential information

Restricts users from sharing high-value data outside of permitted enterprise domains

Manages the movement of sensitive data to address risky behaviours and enforce user controls

Promotes business continuity through the identification and protection of sensitive data

Supports and simplifies regulatory compliance and governance with a highly automated workflow

Reduces the risk of financial penalties, litigation and revenue losses