



SecurEnvoy

A Shearwater Group plc Company

Identity Beyond Boundaries

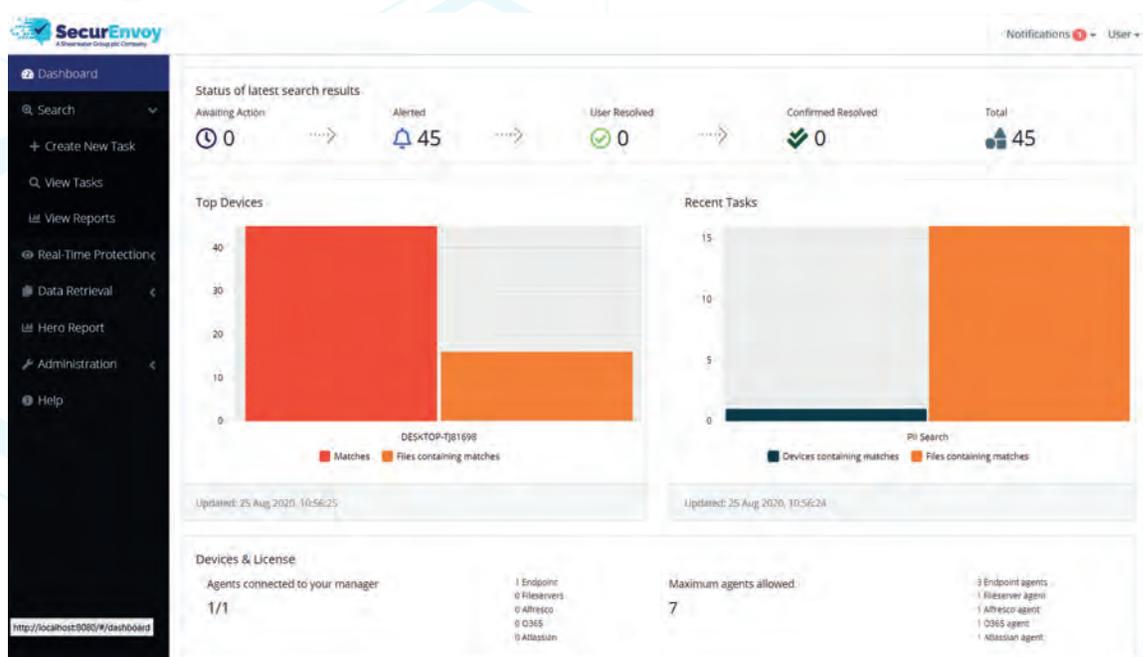
Data Discovery Essentials (DDE)



Introducing SecurEnvoy Data Discovery Essentials

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. This leads 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.

SecurEnvoy Data Discovery Essentials is a highly automated, easy to deploy and use solution for monitoring, classifying, and protecting confidential and sensitive information. Data can be identified across enterprise authorised applications – on premise, in the cloud or hybrid.

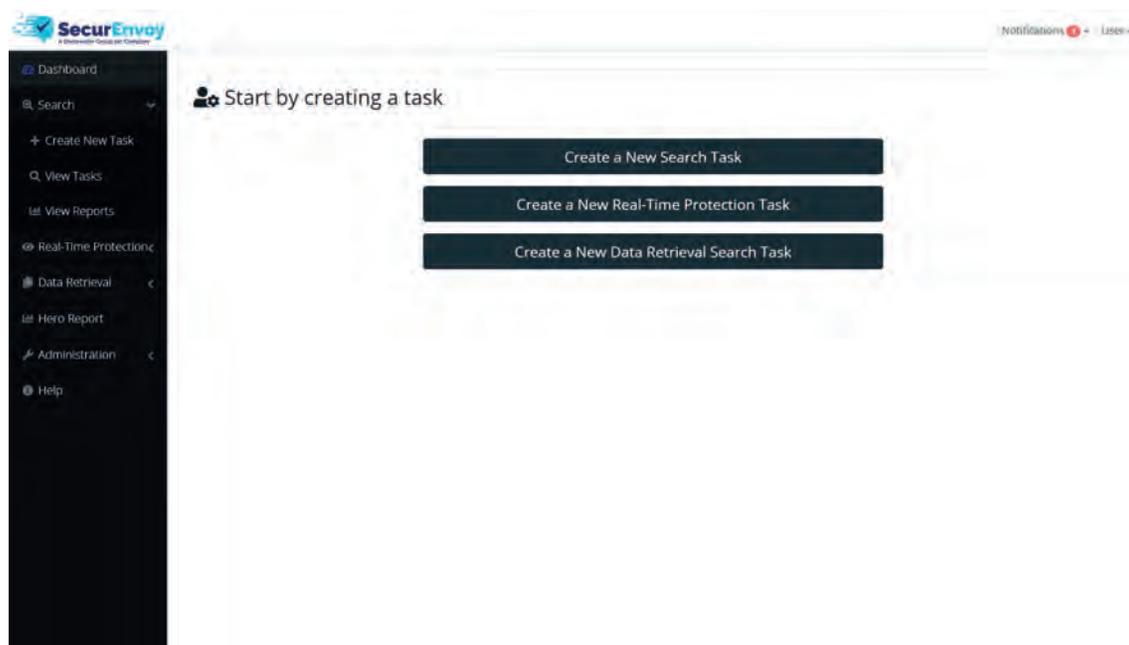


Award Winning and Accurate Content Level Protection

Utilising our patented fingerprinting, classification and machine learning algorithms to protect critical content across your digital estate in real time. SecurEnvoy Data Discovery Essentials 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.

What is SecurEnvoy Data Discovery Essentials (DDE)?

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 SecurEnvoy Data Discovery Essentials (DDE) 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.



SecurEnvoy DDE identifies sensitive and regulated data at rest. 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.

Two Components of Data Discovery

Endpoint Manager

A user interface to manage search tasks, devices, users, licence and other areas of SecurEnvoy DDE, and is shipped as an .exe file. The minimum requirements for this are a Windows 7+ machine, with 8GB of memory and 2 CPUs, as well as the latest versions of Chrome, Firefox or Internet Explorer 11.

Endpoint Agent

It is 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, and the .msi files can be deployed using systems such as GPO and SCCM.



Data Discovery Module

Key Features

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 at-rest

Automated and flexible end user or administrator remediation

Active, passive, stealth and forensic modes

Data Extraction Module

Key Features

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

Data Discovery and Data Extraction - Key Features

- Simple and elegant to deploy and use
- Highly automated remediation capabilities
- Easy data discovery and extraction
- Dynamically generated board level reporting



Data Discovery and Data Extraction - 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.



Identity Beyond Boundaries

Let's Talk.

Global Hubs

LONDON BASINGSTOKE

CHICAGO MUNICH

SALES

sales@securenvoy.com

WEBSITE

www.securenvoy.com

SecurEnvoy is a wholly owned subsidiary of the London Stock Exchange listed digital resilience group, Shearwater Group plc. LSE: SWG



SecurEnvoy HQ, 1 King William St, London EC4N 7AF
Company No. 04866711 VAT Number GB 862076128

Trading Subsidiaries

SecurEnvoy Ltd
SecurEnvoy GmbH
SecurEnvoy Inc.